全国计算机技术与软件专业技术资格（水平）考试参考用书

网络工程师考试同步辅导

（网络系统设计与管理篇）

全国计算机技术与软件专业技术资格（水平）考试办公室推荐

吴 鹏　方 群　高一鸣　主编

清华大学出版社

全国计算机技术与软件专业技术资格（水平）考试参考用书

网络工程师考试同步辅导

网络系统设计与管理篇

全国计算机技术与软件专业技术资格（水平）考试办公室推荐

吴 鹏　方 群　高一鸣　主编

清华大学出版社
北京

全国计算机技术与软件专业资格(水平)考试真题及答案

2008 年下半年试题分析与解答 软考指定用书 清华出版(含各科)

2008 年上半年试题分析与解答 软考指定用书 清华出版(含各科)

2007 年下半年试题分析与解答 软考指定用书 清华出版(含各科)

2007 年上半年试题分析与解答 软考指定用书 清华出版(含各科)

2006 年下半年试题分析与解答 软考指定用书 清华出版(含各科)

2006 年上半年试题分析与解答 软考指定用书 清华出版(含各科)

2009 年计算机技术与软件水平考试各科目考试大纲汇总

全国计算机技术与软件专业资格(水平)考试真题及答案汇总

[软考视频]计算机技术与软件专业资格考试推荐视频教程下载汇总

教材及同步辅导见下页。

计算机技术与软件专业技术(水平)考试指定教材及同步辅导

软考初级：

程序员教程(第二版)2007 版 软考指定用书 高清PDF版

程序员考试辅导：全国计算机技术与软件专业技术资格(水平)考试辅导用书

网络管理员教程(第 2 版)2007 版 软考指定用书 高清PDF版

网络管理员考试同步辅导(计算机与网络基础知识篇) 软考指定辅导用书

网络管理员考试同步辅导(网络系统管理与维护篇) 软考指定使用辅导用书

软考中级：

网络工程师教程(第 2 版) 2007 版 软考指定用书 高清PDF版

网络工程师教程 软考指定用书 高清PDF版

网络工程师考试同步辅导：计算机与网络知识篇 软考指定用书

网络工程师考试同步辅导(网络系统设计与管理篇) 软考指定辅导用书

软件设计师教程(第 2 版) 2007 版 软考指定用书 高清PDF版

软件设计师考试同步辅导(下午科目) 高清PDF版

软件设计师考试同步辅导(上午科目) 高清PDF版

软件设计师考试考点分析与真题详解(软件设计技术篇)

软件设计师考试辅导：考点精讲、例题分析、强化训练 冶金工业出版

数据库系统工程师教程 软考指定用书 高清PDF版

软件评测师教程 软考指定教材 高清PDF版

信息系统管理工程师教程 软考指定用书 高清PDF版

信息系统监理师教程 软考指定用书 高清PDF版

软考高级：

系统分析师教程 软考指定教材 高清PDF版

系统分析师考试辅导(2007 版) 软考指定辅导用书 高清PDF版

系统分析师教程 PDF文字版

系统分析师经典教材 Word版

信息系统项目管理师教程 软考指定教材 高清PDF版

信息系统项目管理师辅导教程(上下册)

计算机专业英语教程 PDF文字版

内 容 简 介

本书按照人事部、信息产业部最新颁布的全国计算机技术与软件专业技术资格(水平)考试大纲和指定教材编写。全书共分为 10 章，内容包括：网络系统的需求分析和设计、构建和测试、运行和维护、管理和评价，以及网络协议、网络设施、网络应用服务、网络新技术等，主要从考试大纲要求、考点辅导、典型例题分析和专项习题训练几个方面对各部分内容展开讲解。

本书具有考点分析透彻、例题典型、习题丰富等特点，非常适合考生在备考时使用，也可作为高等院校或培训班的教材。

图书在版编目(CIP)数据

网络工程师考试同步辅导(网络系统设计与管理篇)/吴鹏，方群，高一鸣主编.
—北京：清华大学出版社，2005.6
(全国计算机技术与软件专业技术资格(水平)考试参考用书)
ISBN 7-302-11110-3

Ⅰ.网…　Ⅱ.①吴…②方…③高…　Ⅲ.计算机网络—工程技术人员—资格考核—自学参考资料　Ⅳ.TP393

中国版本图书馆 CIP 数据核字(2005)第 054268 号

出 版 者：清华大学出版社　　地　　址：北京清华大学学研大厦
　　http://www.tup.com.cn　　邮　　编：100084
　　社 总 机：010-62770175　客户服务：010-62776969
组稿编辑：章忆文
文稿编辑：刘　颖
封面设计：孟繁聪
排版人员：李月菊
印 刷 者：北京国马印刷厂
装 订 者：三河市李旗庄少明装订厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　印张：17.75　防伪页：1　字数：422 千字
版　　次：2005 年 6 月第 1 版　2006 年 3 月第4 次印刷
书　　号：ISBN 7-302-11110-3/TP·7347
印　　数：11001～15000
定　　价：26.00 元

前　言

全国计算机技术与软件专业技术资格(水平)考试举办已经历了十多年，其权威性得到社会各界的广泛认可。为了适应当前信息技术的飞速发展，同时为了更好地服务于考生，本书以2004年新版网络工程师(原网络设计师)考试大纲为依据，严格按照全国计算机技术与软件专业技术资格(水平)考试指定用书——《网络工程师教程》的结构编排，兼顾计算机技术发展和知识更新，细化各章节的基础知识要点，配以真题与典型例题并加以详细剖析。

2004年版新大纲对知识面的要求更宽，更注重实践能力，要求考生在对网络技术知识全面掌握的基础上，建立各种网络技术领域综合应用的思想。同时，考试大纲中还增加了对标准化、信息化、知识产权、法律法规等方面的要求。网络工程师不但要熟练掌握网络体系的基本结构，还要掌握实际组网建设中的设计和实施方法；不但要深入理解网络操作系统以及各种网络应用技术和服务机制，还要能熟练运用网络设备的软硬件配置和管理的各种参数和命令。考虑到网络工程师考试要求的内容多、覆盖的范围广，本书针对网络工程师下午考试所涉及的知识领域的各考点加以系统的阐述。本书章名、节名与信息产业部最新指定教程相同，每一小节分4个板块：考点辅导、典型例题分析、同步练习、同步练习答案。其中，考点辅导部分主要以专题的方式，重点介绍网络工程师下午考试所需的各个方面的知识；典型例题分析是本书的重点，书中的例题一部分是历年网络工程师(原网络设计师)考试真题，另一部分是根据最新考试大纲精心设计的，具有典型性和代表性，并且所有例题均给出了详尽的分析；每章均配有一定数量的习题及答案，对读者所学的知识和能力起到巩固、拓宽和提高的作用。

本书由吴鹏、方群、高一鸣主编。其中第1至6章由方群编写，第8章、第9章由高一鸣编写，第7章、第10章和附录部分由吴鹏编写，另外，参与本书编写和资料整理工作的还有解凯、曹瑶、周晓云、师仁松、汪韵瑶、吴杰、葛世俊、吴晓民、邓金莉、杨明、杨萍、吴婷、谢波、刘瀚、刘菁等。

在本书编写的过程中，参考了许多相关的书籍和资料，在此对这些参考文献的作者表示感谢。

由于时间仓促和水平有限，书中难免存在错漏和不妥之处，敬请读者批评指正。

编　者

前言

目　录

第 1 章　网络系统的需求分析

大纲要求：

- 应用需求分析　包括应用需求的调研(应用系统性能、信息产生和接收点、数据量和频度、数据类型和数据流向等)以及网络应用的分析。
- 现有网络系统分析　包括现有网络系统结构调研(服务器的数量和位置、客户机的数量和位置、同时访问的数量、每天的用户数、每次使用的时间、每次数据传输的数据量、网络拥塞的时间段、采用的协议、通信模式)以及现有网络体系结构分析。
- 需求定义　包括功能需求(待实现的功能)、通信需求(期望的通信模式)、性能需求(期望的性能)、可靠性需求(希望的可靠性)、安全需求(安全性标准)、维护和运行需求(运行和维护的费用)和管理需求(管理策略)。

1.1　网络系统的需求分析

1.1.1　考点辅导

1.1.1.1　应用需求分析

1. 应用需求的调研

需求分析是构建网络的第一个阶段，通过需求分析，可以帮助网络设计者更好地理解网络功能、更好地评价现有网络、更客观地做出决策，有助于提供更加完善的交互功能和移植功能，更合理地使用用户资源等。

应用需求的调研内容包括应用系统性能、信息产生和接收点、数据量和频度、数据类型和数据流向等。

(1) 应用系统性能

用户系统中的应用有许多类型，其中一些应用在整个系统中占有相当重要的地位。应用系统的性能往往是用户最为关注的，常见的性能指标包括：可靠性/可用率、响应时间、安全性、可实现性和实时性等。

(2) 信息产生和接收点

网络上的信息流都有其产生和接收的位置，产生信息的称为源，接收信息的则称为宿(即目的)。在进行需求分析时分清信息的源和目的是非常必要的。

(3) 数据量和频度

网络中的通信类型包括数据、视频信号和音频信号等，不同类型的流量使用不同的量度，数据的流量一般用平均或高峰时每秒传送的位数(比特每秒，简写为 b/s)表示。视频信号的流量用电视通道数表示，每个通道占 6MHz 带宽，音频信号则用欧拉数表示。

频度指数据在单位时间内传送的次数，不同类型的数据传送的频度不同。

流量估计应该先分析用户的网络应用，分别估计每种应用产生的分流量，再把各种分流量乘以频度累计得出系统的总流量。

准确的流量估计可以避免网络系统因带宽过窄而形成瓶颈，导致网络吞吐量和性能的下降，因此对网络通信业务量的估计必须留有足够的余量。

(4) 数据类型和数据流向

网络服务一般分为 3 种：共享数据服务、综合语音服务和多媒体应用服务。其中共享数据服务是最常见的业务，综合语音服务主要是电话类业务，而多媒体应用服务则包括语音、图形、图像等多种服务，不同的服务有不同的数据类型。

数据流向是指数据流传输的方向，在客户机/服务器工作模式中，数据的流向既可以是客户机到服务器的，也可以是服务器到客户机的。

因此，网络设计人员必须根据用户具体的应用情况，详细分析网络承载的数据类型和数据流向，合理分配网络容量。

2. 网络应用的分析

网络的主要功能是通过数据传输实现数据共享，目前应用在科研、教育、金融证券、企业管理、制造、办公自动化、电子商务、家庭娱乐等许多领域。

网络应用按照响应时间可以分为两种：实时应用和非实时应用。不同的应用有不同的网络响应性能需求，对网络延迟和带宽有不同的影响。

实时应用要求将节点机产生的数据立即传送出去，一般不需要用户干预。实时应用要求信息传输的速率稳定，具有可预测性。令牌传递网络(令牌环网或 FDDI)和面向连接的服务(如 ATM)可以为这些应用提供支持，但在网络分析与设计中通常不考虑实时应用。

通常所说的应用指的是非实时应用，此类应用对网络带宽和数据传输能力要求比较高，当暂时争用不到网络介质时，只要介质可以承受任何突发性的数据收发任务，非实时应用就不会出现问题。所以，这种应用适合于类似于以太网的共享介质网络中。

另外，按照应用是否共享，又可以把应用分为独立应用和共享应用两种类型。

不同的应用对网络功能和性能方面的需求不同，网络设计人员应对网络应用需求加以分析，确定网络的应用目标及其他相关指标。

1.1.1.2 现有网络系统分析

1. 现有网络系统结构调研

如果需要在已有网络上构建新系统，那么就应该全面了解现有网络情况，尽可能考虑旧系统的利用，这样既可保护用户原有投资，又能让用户在使用新系统时有一个平滑的过渡，从而大大节省培训的时间和费用。

网络系统的建设一般需要分成几个阶段来实施，每个阶段都是在前期网络的基础之上进行的，不可能完全抛弃现有网络。因此，必须对现有网络进行仔细调研，以考查在原有网络中哪些部分是可以利用的，哪些是需要升级的，哪些是无用而必须舍弃的。重点考查以下几个方面：

(1) 服务器的数量和位置

服务器是网络中提供专门服务的设备，是网络中的稀缺资源，新网络应该尽量将它们包括进去。在建设新网络之前，需要清楚了解服务器的台数、位置、型号、使用的软件、提供的服务类型以及其他各项性能指标。

(2) 客户机的数量和位置

客户机是用户使用网络服务的窗口，有的客户机只供单个用户使用，而有的则供多人使用(如图书馆的查询机)；另外在客户机上运行的应用系统有差别，对网络服务的需求也不一样。网络中包含客户机的数量及承担的任务决定了网络的负载，因而有关客户机的信息对网络系统的设计也非常重要，新建网络必须仔细考虑它们。

(3) 使用情况

网络的使用情况包括客户机的数量、访问类型、每天的用户数、每次使用的时间、每次数据传输的数据量、网络拥塞的时间段等，这些数据都可以通过查询网络管理系统的日志文件获得，如果没有完整的日志数据，也可以通过与用户交谈获得有用信息，这些数据虽然不需要过分准确，但其准确性将影响到今后网络的设计方案。

(4) 采用的协议

协议是网络通信的基础，原有网络可能包含有多种协议，协议间存在着一定的差异，这需要进行详细的调查，以便新建网络时能够很好地照顾到多种协议间的差异，方便不同协议数据之间的转换。

(5) 通信模式

通信模式就是用户接入网络的方式。网络设计要兼顾到各种通信模式。

2. 现有网络体系结构分析

网络体系结构是定义和描述一组用于计算机及其通信设备之间互联的标准和规范的集合，遵循这组规范就可以实现计算机设备之间的通信。目前有两大主流体系结构标准，一个是国际标准 OSI/RM(开放系统互联参考模型)，另一个是工业标准 TCP/IP 模型。

OSI 参考模型通过分层和抽象，将网络划分为七个功能各异的层次，同一端系统中的低层为高层提供服务，不同端系统中的对等层之间进行通信并交换协议数据单元。它是一个开放系统模型，概念清晰，但偏重于理论研究，复杂而不实用，目前实现的范例还较少。

TCP/IP 简化了 OSI 参考模型的分层结构，层次明显减少，实现简单，功能强大，目前为大多数厂商支持，已成为网络通信协议事实上的标准，并已得到普遍的推广。其他还有 SNA 和 DNA 等著名的体系结构。

通过对现有网络体系结构的分析，为建设新网络提供参考依据，同时在设计新网络时也应该照顾到原有网络的体系结构，尽量发挥其优势，而不应该完全抛弃。

1.1.1.3　需求定义

网络系统的需求包括功能需求、通信需求、性能需求、可靠性需求、安全需求、维护和运行需求以及管理需求等，下面逐一介绍。

1. 功能需求

功能需求即是网络在用户单位业务中应该提供的功能，可以通过了解用户单位所从事的行业，该单位在行业内的地位以及和其他单位的关系等来确定功能需求。另外还可通过

了解项目背景，明确用户单位建网的目的，从而有助于描述详细的功能需求。

2. 通信需求

在网络中，网络通信是个人通信模式和流量的组合。通信模式又以发生在节点之间的通信方式为基础。通信方式有如下几种：

- 对等通信方式
- 客户机/服务器通信方式
- 服务器/客户机通信方式

独立节点之间可以在一种或多种方式下通信，如何选择通信方式取决于网络的资源、节点和应用程序的性能。例如，在对等通信方式下，各工作站之间可共享资源；在客户机/服务器通信方式下，可以访问中央文件服务器上的核心数据库。

(1) 对等通信方式

对等通信方式是在一种结构和功能相似的节点(客户机)之间的通信，通信节点具有相似的应用和通信能力。在该种网络中，每个节点与网络中的其他节点相连接，没有明显的源通信模式和目的通信模式。

(2) 客户机/服务器通信方式

客户机/服务器通信方式是网络中的客户机和服务器之间的通信。客户机可以是任何类型的节点，这些节点可访问一些共享的资源。服务器在大小和功能上有所不同，既可以是基于 PC 机的服务器，也可以是中型计算机和大型计算机。

(3) 服务器/客户机通信方式

数据库服务器应用程序使数据从服务器流向客户机。通常情况下，客户机请求比服务器响应所传送的通信量要少。例如在典型的 Web 方案中，服务器根据客户机浏览器的请求向客户机发送大量的 Web 页面，这就是所指的服务器/客户机分布。

(4) 相关指标

为了确定用户的通信需求，需要了解用户单位的建筑物布局、入网站点的分布情况，并记录下述信息：

- 网络中心(或计算中心)及各级设备间的位置。
- 用户数量及其位置。
- 任何两个用户之间的最大距离。
- 用户群组织(即在同一楼里或同一楼层里的用户，尤其注意那些地理上分散，却属于同一部门的用户)。
- 特殊的需求或限制(例如网络覆盖的地理范围内是否有道路、山丘；建筑物之间是否有阻挡物；电缆等介质布线是否有禁区；是否存在可以利用的介质系统等)。

3. 性能需求

在需求分析中要分析网络的多种性能特性，它们是：响应时间、延迟、等待时间、利用率、带宽、容量、吞吐量、可用性、可靠性、可恢复性、冗余度、适应性、可伸缩性、效率和费用等，有些需求用户不是很关心，但对于设计者却是必须考虑的。

随着计算机网络数量的增长、规模的扩大，如何提高网络性能成为十分重要的问题。与衡量单机系统的性能不同，网络性能是衡量一群计算机系统的性能。了解网络用户的需要，设定恰当的性能目标，合理选择网络结构和组成，便能得到满足用户需求且性能比较好的网络。

网络用户关心的网络性能是能否获得最快的响应，网络管理员关心的网络性能是能否获得最高的资源利用率，两者需要很好的平衡。这种平衡包括两个方面：一方面是性能和价格的折中；另一方面是吞吐量和响应时间的平衡。

4. 可靠性需求

可靠性需求就是用户需要什么样的可靠性。一个系统的可靠性定义为在指定的条件和时间内，系统能够实现指定功能的概率。而整个系统的可靠性又取决于组成系统的各个部件的可靠性。

可靠性指标一般包括平均无故障时间(MTBF)和平均修复时间(MTTR)、可用性和故障率等。

5. 安全需求

(1) 安全需求概述

网络安全性包括对物理产品的布局和对过程的操作，这样可以保护网络和系统的完整性、可行性及可靠性。现代的网络安全性是把基本的网络安全性概念运用在分布式网络环境中。网络安全性的目的是对资源的保护，目前还没有彻底的解决方法。

安全设计包括安全服务和实施两方面。原则上讲，每一个网络系统都具有独立和通用的安全协议，而基于安全服务的安全信息则是存放在管理信息库(MIB)中的，只有授权人员或系统才可访问、修改或删除这些机密信息。通过对网络易损点的识别，可使这些易损点得到保护和监控，要确保安全应采取一种分层管理策略。

安全性策略的 3 个属性定义为保密性、完整性和可信性。信息损失通常由以下原因引起：更改、破坏、泄露。对网络安全构成威胁的形式有很多，而且它们常导致网络失常和重要信息的毁坏。

采取何种安全措施需要视用户需要而定，不同单位或一个单位的不同部门要求的安全等级往往是有差异的，并不是安全等级越高越好，较高的安全等级意味着额外的系统开销和高昂的费用。

(2) 安全性标准

网络系统是否达到一定的安全性主要依照相关的安全性标准来判断，最早的信息系统安全性标准由美国国防部颁布的黄皮书(TC-SEC-NCSC，可信计算机系统)规定。该手册将 IT 系统划分为 A(A1)、B(B1、B2、B3)、C(C1、C2)、D(D1)共 4 类 7 个安全等级。

① D 类安全等级　D 类安全等级只包括 D1 一个级别，D1 的安全等级最低，它只为文件和用户提供安全保护。D1 系统最常见的形式是本地操作系统，或者是一个完全没有保护的网络。

② C 类安全等级　该类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1 和 C2 两类。

③ B 类安全等级 B 类安全等级可分为 B1、B2 和 B3 三类。B 类系统具有强制性保护功能，这就意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。

④ A 类安全等级 A 类系统的安全级别最高。目前，A 类安全等级只包含 A1 一个安全类别。A1 类与 B3 类相似，对系统的结构和策略不作特别要求。A1 系统的显著特征是：系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析后，设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足下列要求：系统管理员必须从开发者那里接收到一个安全策略的正式模型；所有的安装操作都必须由系统管理员进行；系统管理员进行的每一步安装操作都必须有正式文档。

欧洲等价的分类手册是 ITSEC(信息技术安全评估标准)，与美国的黄皮书类似，ITSEC 标准目录将 IT 系统划分为 7 个安全等级(E0~E6)，与黄皮书中的各个等级大致对应。

6. 维护和运行需求

维护与运行是网络系统投入正常运行后的日常管理工作，这项工作主要由网络管理人员承担。网络管理人员通过网络管理系统可以完成系统的配置、监控和统计等事务的处理，有时还要对网络设备进行检修。网络设计人员需要根据用户需求，提供必要的网络管理工具和策略，方便网络管理员对整个网络进行管理和维护，提高网络运行效率，保证网络的可靠性。

7. 管理需求

从用户的角度讲，一个网络管理系统应该满足以下要求：

- 同时支持网络监视和控制两方面的能力。
- 能够管理所有的网络协议。
- 尽可能大的管理范围。
- 尽可能小的系统开销。
- 可以管理不同厂家的联网设备。
- 容纳不同的网络管理系统。
- 网络管理的标准化。

在 OSI 网络管理框架模型中，基本的网络管理功能被分为 5 个功能域：配置管理(Configuration Management)、性能管理(Performance Management)、故障管理(Fault Management)、安全管理(Security Management)和计费管理(Accounting Management)。

网络管理的标准化产品包括 ISO 的 CMIS/CMIP(Common Management Information Service/Common Management Information Protocol)、Internet 体系结构委员会 IAB(Internet Architecture Board)的 SNMP 和管理信息库 MIB，这些内容将在第 5 章详细介绍。

1.1.2 典型例题分析

例 1 网络工程是一项复杂的系统工程，一般可分为网络规划、网络设计、工程实施、系统测试验收和运行维护等几个阶段。网络规划是在需求分析的基础上，进行系统可行性分析和论证，以确定网络总体方案。网络规划阶段任务完成之后转入下一阶段，即网络设计阶段。(2001 年下午试题第二题)

【问题】

1. 简述网络规划阶段需求分析的方法和解决的问题(控制在 100 个字以内)。

2. 在需求分析过程中应对已有网络的现状及运行情况作调研，如果要在已有的网络上作新的网络建设规划，如何保护用户已有投资(控制在 100 个字以内)?

分析：需求分析可以采用自顶向下的分析方法，了解用户单位所从事的行业、地位及和其他单位的关系等。了解项目背景，有助于更好地了解用户单位建网的目的和目标。

对用户单位的建网目的和目标进行分析之后，应进行纵向的、更加细致的需求分析和调研，从而明确以下 6 个方面的情况:

(1) 地理布局。了解用户单位的建筑物布局，入网站点的分布情况。

(2) 用户设备类型。

(3) 网络服务。

(4) 通信类型和通信量。

(5) 容量和性能。网络容量是指在任何时间间隔，网络能承担的通信量。网络性能一般用经过网络的响应时间或端到端时延表示。

(6) 网络现状。尽可能在设计新系统的时候考虑旧系统的利用，既可保护用户投资，又能够使用户在系统的使用上有一个平滑过渡，节省培训时间和费用。

答案:

1. 先采用自顶向下的分析方法。调查用户单位建网的背景、必要性、上网的人数、信息量等，从而确定建网目标。接着进行纵向的、深入的需求分析和调研，为网络设计提供依据。

2. 在设计新系统时要充分考虑到利用已有系统的资源，让原有系统纳入到新系统中运行，不要“推倒重来”。也可以把已有系统的设备降档次使用。

例 2　网络开发设计的整个过程分为哪几个阶段？每个阶段有什么任务？请用流程图的方式说明。

分析：网络开发过程根据任务的不同可分为以下 5 个阶段:

阶段 0: 产品概念和机会评估。包括概念回顾、把概念与战略意图进行比较、决定是否进入阶段 1，生成最初的合同等文档。

阶段 1: 网络需求与商业计划。编制网络需求说明书、编制通信规范、识别主要的设计要素，生成网络需求说明书和通信规范等文档。

阶段 2: 网络分析、设计和实施。编制逻辑和物理说明书、确定战略，生成项目计划、逻辑设计图和物理设计图等文档。

阶段 3: 综合。购买硬件和软件、独立或指导下的新系统测试，生成测试结果报告文档。

阶段 4: 实施和运行。整个系统的实施，生成项目完成报告等文档。

答案:

网络开发的过程一般分为 5 个步骤，如图 1.1 所示。

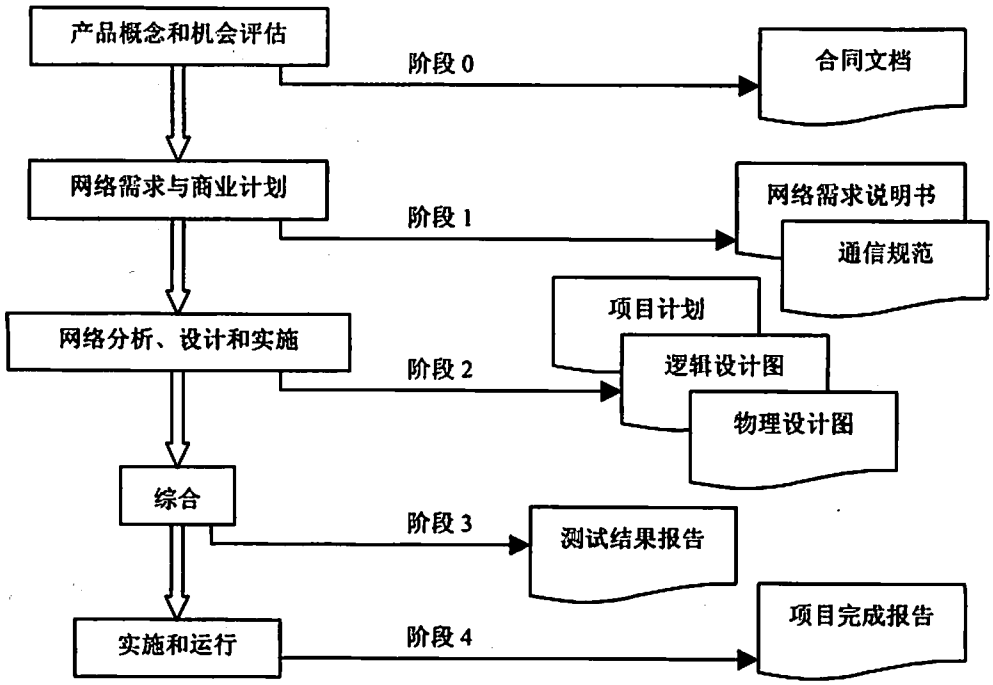


图 1.1 网络开发过程浏览

例 3 网络的性能主要体现在哪几个方面?

分析:网络的性能中有如下一些指标是必须考虑的,它们标识着整个网络的性能:

(1) 响应时间、延迟和等待时间

响应时间指的是从服务器发出请求开始到接收到相应的响应所花费的时间,它经常用来评价终端向主机交互式地发出请求信息所花费的时间。响应时间是数据通过网络中的每一部分所花费时间之和。每一个设备,通信连接以及处理过程的自身延迟都会影响整个响应时间。在客户机/服务器网络结构中,响应时间指的是服务器响应客户工作站提出的请求所花费的时间。另一个影响响应时间的因素是网络延迟,当请求/应答通信流通过公共广域网的时候,响应时间就会发生很大变化。

(2) 利用率

利用率反映出指定设备在使用时所能发挥的最大能力。在网络分析与设计过程中,通常考虑以下两种类型的利用率:CPU 利用率和链路利用率。

CPU 利用率是指在处理网络发出的请求和做出响应时处理器的繁忙程度。网络设备互联(如路由器)要处理的数据包越多,则所耗费的 CPU 时间越长。由于 CPU 的处理能力一定,如新的工作需要更快的 CPU,则有些工作就必须排队等待。

链路利用率指的是链路总带宽的有效使用百分比。例如,购买了一条 T1 线路,它有 24 条信道,最大带宽为每条信道 64Kb/s,如果只利用了 6 条信道,则这条线路的利用率就是 64Kb/s × 6 = 384Kb/s,即最大带宽的 25 % (384Kb/s/(64Kb/s × 24))。

(3) 带宽、容量和吞吐量

带宽是指通过通信线路或通过网络的最高频率与最低频率之差。带宽对于模拟信号网

络而言，其单位为赫兹(Hz)；对于数字信号网络而言，其单位为比特/秒(b/s)。

容量指的是通信信道或通信线路的最大数据传输能力。它经常用来描述通信或连接的能力。例如，一条 T1 通道的容量是 64Kb/s。

吞吐量是指在网络用户之间有效地传输数据的能力。吞吐量常用来评估整个网络的性能，对吞吐量进行量度的一种有效方法是信息比特吞吐率(TRIB)，有效的吞吐量与响应时间是直接相关的，有效吞吐量越高，响应时间越快。

(4) 可用性、可靠性和可恢复性

可用性是指网络或网络设备(如主机或服务器)可用于执行预期任务的时间的总量(百分比)。

可靠性是网络设备或计算机持续执行预定功能的可能性。可靠性经常用平均故障间隔时间(MTBF)来量度。这种可靠性量度也适用于硬件设备和整个系统。它表示了系统或部件发生故障的频率。

可恢复性是指网络从故障中恢复的难易程度和时间。可恢复性即指平均修复时间(MTTR)。平均修复时间用来估算当故障发生时，需要花多长时间来修复网络设备或系统。可用性计算公式如下：

$$A=MTBF/(MTBF+MTTR)$$

(5) 冗余度、适应性、可伸缩性

冗余度是指为避免停机而为网络增加双重通道和设备。冗余度是另一个在网络设备和系统设计与实施中需要考虑的因素，是指在城域网(MAN)或广域网(WAN)中提供备用的路径来传输信息。当原来的链路中断后，备用的路径将会发挥作用。

适应性是指在用户改变应用要求时网络的应变能力。

可伸缩性是指网络技术或设备随着用户需求的增长而扩充的能力。

(6) 效率与费用

效率是指网络如何更有效地使用所提供的带宽。

网络费用是指与传输的用户数据相关的协议信息的数量。

答案：略。

1.1.3 同步练习

1. 网络系统的需求分析的目的是什么？对以后的工作有何指导意义？
2. 如何确定用户的需求？
3. 如何进行计算机网络安全需求分析？

1.1.4 同步练习参考答案

1. 需求分析有助于设计者更好地理解网络应该具有什么功能和性能，最终设计出符合用户需求的网络，它给设计者设计一个网络提供了以下的依据。

- 能够更好地评价现有的网络体系。
- 能够更客观地做出决策。

- 提供完美的交互功能。
- 提供网络的移植功能。
- 合理使用用户资源。

2. 确定用户需求的步骤：收集需求→列出服务需求→列出性能需求→编制需求说明。

3. 面对各种网络安全威胁，为了帮助企事业机构正确制定出网络安全防范策略，网络管理员必须首先对网络的实际安全状况和企业应用需求进行分析。大致包括以下几个方面：

(1) 明确网络资源

应充分了解网络的拓扑结构，包括网络中使用了哪些设备，其型号和生产厂商，在网络中安装的位置，是否能够正常工作，设备的性能及配置操作，允许和禁止的访问，另外如何协调网络资源以实现这些访问等。

(2) 确定网络访问点

了解整个网络系统的所有可能接入点，以及这些可接入点访问系统资源的路径，能接触这些可接入点的人员等。

(3) 确定访问范围与权限

根据员工的工作职责范围表，网络管理员可以确定每个网络用户所需要的网络资源访问范围和权限。以此为依据，可以制定出用户访问网络资源的权限约束。

(4) 确认安全隐患

网络管理员必须认真分析网络设计方案，认真建立、记录、保存和检查网络系统的运行档案，从网络的日常运行中发现潜在的安全隐患和漏洞。

(5) 人为因素对网络安全的影响

在网络安全体系结构构建的过程中，人为因素对网络安全的影响也非常重要。即使是网络管理员已经制定了相对完善的安全制度，如果操作人员不按照规程操作或违反规定进行某些越权操作，仍将造成安全威胁。

因此，从以上几个方面着手，对现有系统进行安全需求分析，才能为网络系统规划和设计提供必要的安全依据。

1.2 本章小结

本章主要介绍了构建网络前期准备工作中重要的一环——需求分析，网络需求分析包括对现有网络的调研和分析，以及用户对新建网络的预期需求，其中又包括功能需求(待实现的功能)、通信需求(期望的通信模式)、性能需求(期望的性能)、可靠性需求(希望的可靠性)、安全需求(安全性标准)、维护和运行需求(运行和维护费用)和管理需求(管理策略)等。做好需求是组建新网络工程的第一步，也是最重要的一步。

第 2 章　网络系统的设计

大纲要求：

- 技术和产品的调研和评估　收集信息，采用的技术和产品的比较研究。
- 网络系统的设计　确定协议，确定拓扑结构，确定连接(链路的通信性能)，确定节点(节点的处理能力)，确定网络的性能(性能模拟)，确定可靠性措施，确定安全性措施(安全措施的调研、实现安全措施的技术和设备的评估)，网络设备的选择，制定选择标准(成本、性能、容量、处理量、延迟)，性能指标的一致性。
- 新网络业务运营计划　业务过程的确认，安装计划，转换到新网络的计划。
- 设计评审。

2.1　网络系统的设计

2.1.1　考点辅导

2.1.1.1　网络设计的基本原则

网络系统性能要求高、技术复杂、涉及面广，在其规划和设计过程中，为使整个网络系统更合理、更经济、性能更好，需要遵守以下设计原则：性价比高、统一建网模式、统一网络协议、保证可靠性和稳定性、保证先进性和实用性、具有良好的开放性和扩充性、在一定程度上保证安全性和保密性、具有良好的可维护性等。

由于不同单位的网络发展水平和应用需求差异很大，而且网络的组网方法和备选设备种类繁多，因此设计时必须根据具体情况进行规划。

2.1.1.2　收集信息

在网络开发过程中，一旦设计者了解网络需求之后，便可进入逻辑网络设计阶段。进入这一阶段的前提是设计者必须有详尽的需求报告和通信规范。

在网络设计的初始阶段，网络设计人员首先要对用户的需求了如指掌，然后着手进行网络设计前的准备工作。准备工作首先从收集信息开始(这些信息包括技术层面的和产品层面的)收集信息一定要以满足用户需求为目标，为网络设计和实施服务。

收集信息的途径有很多种，主要有：

- 通过参观访问其他单位获得。
- 通过厂商资料和宣传品获得。
- 通过 Internet 获得。
- 通过投标公司获得。

- 通过其他渠道获得。

收集到的信息需要分类整理，参照需求分析说明书找到可靠的且满足需要的技术、产品和设备，然后进一步分析研究。

2.1.1.3 采用的技术和产品设备的比较研究

任何设计都需要权衡，其中最常见的是成本与性能的权衡。如果要增强性能，成本就会明显上升。在考虑成本时，设计者不仅要考虑运行的成本，还要考虑实施网络的成本。图 2.1 说明了技术选择与成本之间的关系。

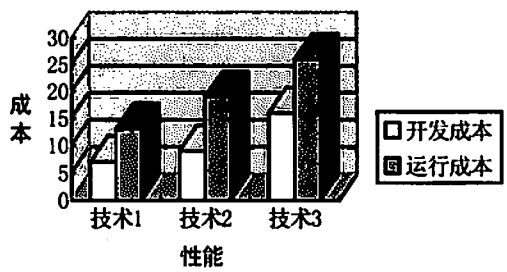


图 2.1 成本/性能示意图

根据需求收集阶段初期收集到的基本需求，可以预测项目的成本，同时也可确定开发成本和运行成本的阈值。在选择技术时，设计者通常也会提供备选的技术及相关的成本，选择的结果一般会超出所确定的水平。给定一个设计目标时，设计者必须考虑以下方面：

- 最低的运行成本。
- 最少的安装费用。
- 最高的性能。
- 最大的适应性。
- 最大的安全性。
- 最高的可靠性。
- 最短的故障时间。

以上目标不可能同时达到，需要仔细权衡。其中技术上的考虑处于核心地位，技术上的考虑包括后台通信、连接类型和可伸缩性等方面。

1. 后台通信

后台通信通常是指广播通信，与应用间的通信不同，它是发生在网络上的通信。考虑后台通信是因为它可能大大地增加网络的容量要求。在典型的情况下，后台通信占全部通信的 5%~20%。

通常遇到的后台通信基于路由广告协议(Routing advertIsements Protocol，RIP)和服务广告协议(Service Advertisements Protocol，SAP)。在网络上向其他设备做服务广告的服务器、路由器和打印机将产生这种类型的通信。如果网络协调不当，后台通信就会在整个网络通信中占很大一部分。

2. 连接类型

连接类型是逻辑设计时必须考虑的另一个问题。在无连接和面向连接的协议间需要一个权衡。有些协议，比如 IP 协议是无连接的，在这类协议中，不用花时间来建立虚拟电路，只是简单地通过网络来发送分组。用无连接协议传送信息比起面向连接的协议来说，每个分组的系统花费都要多些。

面向连接的协议(比如 ATM)需要花较长时间建立连接。一旦建立了连接，通信的效率就会高许多。面向连接的协议通常同时提供多层次的服务，当应用需要以相同的速率发送大量的信息时最适合使用面向连接的协议。如果应用是突发的而且不需要多层次服务，则用非连接协议最合适。

3. 可伸缩性

设计者同样需要考虑网络的可伸缩性，即考虑现在以及将来网络所需的容量。容量设计必须易于调整以适应单位、应用以及网络的适当增长。例如，当设计者实施以太网接口卡(NIC)和非屏蔽双绞线(UTP)连接时，即使只实现 10Mb/s 的以太网，也可能选择购买 10/100Mb/s 的网卡和五类线。这样做，不更换接口卡和线缆平台就能升级到百兆。

要想做出具体的技术选择，需要设计者详细考虑每种方法的相关优缺点。考虑的不同技术类型和重点内容如下：

- 物理层
- 网络互联
- 逻辑网络图
- 虚拟网策略
- 现代广域网技术
- 网络管理
- TCP/IP 地址设计
- 网络安全
- 防火墙
- 备选设计

2.1.1.4　确定协议

从前一章可知 OSI 参考模型各层的任务实际上是通过网络协议实现的。在网络中，“协议”用来指代一组联合作用的单个协议。一组协议中的每个协议均被赋予不同的任务，例如，数据翻译、数据处理、错误校验以及编址，这些协议对应于 OSI 模型的不同层。目前有四种主要的联网协议组：TCP/IP、IPX/SPX、NetBIOS 和 Apple Talk，它们的功能和结构各有异同，图 2.2 显示的是 TCP/IP 协议与 OSI 参考模型不同协议层次的比较。

不同的协议有各自的优点和缺点，使用何种协议(或协议组)依赖于许多因素，包括既有的网络系统、用户单位的技术和专业知识以及网络安全性和速度需要。根据它们的速度、发送效率、资源利用率、安装难易程度、兼容性以及在一个局域网段与另一个局域网段之间的连通能力而使用不同的协议。

除网络规模大小外，还必须考虑它的互联需求，数据安全性需求以及网络管理人员的技术专业知识。大多数网络由于具有混合的硬件或软件体系结构而使用多种协议，因此，

作为网络工程师不仅要了解每种协议，而且要理解它们是如何联合作用的。使用多种协议的网络被称为多协议网络，多协议网络在商业界是非常通用的。

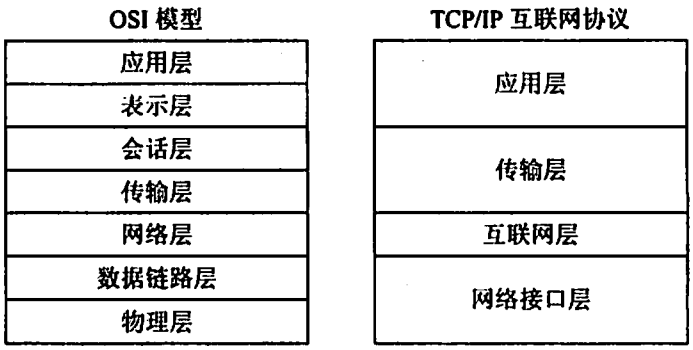


图 2.2 TCP/IP 与 OSI 层次的比较

2.1.1.5 确定拓扑结构

网络拓扑结构设计是网络逻辑设计的第一步，它主要是确定各种设备以什么方式相互连接。在设计时应考虑网络的规模、网络的体系结构、所采用的协议、扩展和升级管理维护等各方面的因素。

一个规模较大的网络系统往往被分为不同层次的多个部分，它们之间既相对独立又互相关联，这就是层次型网络结构设计。使用层次模型设计具有以下好处：减轻网络设备处理器的负载、降低网络成本、简化设计元素、容易调整层次结构、可充分发挥互联设备的特性等。最常见的网络拓扑三层模型结构通常包括核心层、分布层和访问层等 3 个层次。

拓扑结构反映了互联网络的结构映像图，用来指示组成网络的网段、互联点及用户分布。网络拓扑结构说明的是网络的几何形状，而不是它的地理位置或技术实现。在拓扑结构设计阶段，要确定网段和互联点、明确网络的大小和范围以及所需要的网络互联设备类型。常见的网络拓扑结构有星形、总线(树)形、环形和网状及不规则形状等，如图 2.3 所示。

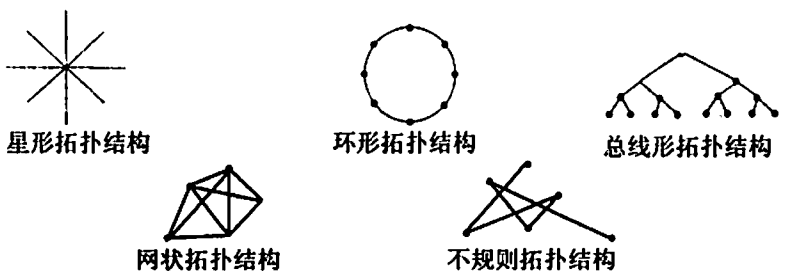


图 2.3 拓扑结构的类型示意图

(1) 星形网

以一台中心处理机为主而构成的网络，其他入网机器仅与该中心处理机之间有直接的物理链路(包括通过集中器和前端机等)，中心处理机采用分时或轮询的方法为入网机器服务，所有的数据必须经过中心处理机向外分发。

(2) 总线(树)形网

所有入网设备共用一条物理传输线路，所有的数据发往同一条线路，并能够由附接在线路上的所有设备感知。设备通过专用的分接头接入线路，由于线路对信号的总衰减作用，总线形网仅用于有限的区域，常用于组建局域网络。

(3) 环形网

入网设备通过转发器接入网络，每个转发器仅与两个相邻的转发器有直接的物理线路。环形网的数据传输具有单向性，一个转发器发出的数据只能被另一个转发器接收并转发。所有的转发器及其物理线路构成了一个环状的网络系统。环形网也是局域网的一种主要组成形式。

(4) 网状网络

利用专门负责数据通信和传输的节点机构成的网络，入网设备直接接入节点机进行通信。网状网络通常利用冗余的设备和线路来提高网络的可靠性，因此，节点机可以根据当前的网络信息流量有选择地将数据发往不同的线路。网状网络主要用于地域范围大、入网主机多(机型多)的环境，常用于构造广域网络。

由于不同拓扑结构的网络往往采用不同的网络控制方法，具有不同的性能，适用于不同的应用环境，因此，可以根据不同的应用需求，选择单一或多种混合的网络拓扑结构。

需要指出的是，从可靠性及易于维护的角度出发，越来越多的网络转向物理上的星形拓扑结构。但由于历史的原因，在数据流向方面仍然保持原有的特点，因此，目前人们常根据数据流向，从逻辑上对网络进行类似的分类。

2.1.1.6 确定连接

除了考虑各种类型网络的传输特性及优缺点，还需要考虑在实际网络环境中如何评估各类介质。以下列举了必须考虑的主要环境因素，并对不同的条件推荐了适当的传输介质。

(1) 高 EMI 或 RFI 区域

如果环境内拥有许多电能源，应尽可能使用抗噪性最好的介质。Thick Ethernet 和光缆在目前是抗噪性最好的介质。

(2) 拐角和狭窄空间

如果环境要求电缆在拐角处弯曲或穿过狭窄空间，应该尽可能使用最灵活的传输介质，如 STP 和 UTP。

(3) 距离

如果环境要求远距离传输，应考虑光缆或无线介质，也可以使用双绞线或同轴电缆，但它们更易受衰减和干扰的影响，同时需要中继器。

(4) 安全性

如果某个机构对传输安全性要求较高，则应选择具有最高安全性的传输介质，光缆和红外介质对这种环境都是很好的选择。

(5) 既有体系结构

如果对一个已有的电缆设备增加电缆，应考虑它将如何与已有电缆设备相互作用以及两者间所需的连接性硬件。选择的介质应与机构以前安装的设备相适应。

(6) 发展

弄清本单位准备如何扩展网络，以及在设计布线时是如何考虑将来的应用、通信业务和地理扩展这些问题的，所选的介质应该能适应机构的需求。

2.1.1.7 确定节点

节点是网络中功能相对独立的部分，它可以发送、接收或转发、处理并存储数据，它可能是一台用户终端或服务器，也可能是一个集线器、交换机或路由器等。在网络设计和规划中需要多少个节点、它们应该如何分布在不同的地理位置、每个节点的处理能力等都必须明确。这就需要网络设计人员综合多种因素考虑，如用户需求、3~5 年后的发展情况、现有网络资源的利用、保证可靠性而采取的冗余措施等。

2.1.1.8 确定网络的性能

网络作为一个系统来看，其性能取决于多种因素，主要包括构成网络的各个部件的性能。从第 1 章内容可知网络的性能包括以下 6 个方面：

- 响应时间、延迟和等待时间。
- 利用率。
- 带宽、容量和吞吐量。
- 可用性、可靠性和可恢复性。
- 冗余度、适应性和可伸缩性。
- 效率与费用。

确定网络的性能就是要针对每一种性能选取适当的指标，以保证在网络工程施工后期测试时有据可依，评判建成的网络是否满足性能设计要求。

总的来说，网络的性能与网络的投入成正比，即选用的组网设备和部件越好，整个网络的性能就越高，但不同的单位有不同的需求，需要在性能和投入两者之间找到一个平衡点，力争做到投入少、性能好。

2.1.1.9 确定可靠性措施

对于一个网络系统来说，可靠性就是对应用程序和数据的有效支持。在实际应用中，提高网络的可靠性的可行方法是消除故障孤点，特别是单点故障。

1. 可靠性设计的内容

可靠性设计包含 3 方面的内容：

(1) 物理可靠 指系统对关键硬件设备(如 CPU、存储介质等)损坏、不可预见性灾难(如地震、飓风、陨石、强磁场等)、对硬件、数据库及服务资源等的破坏的耐受能力。

(2) 逻辑可靠 包含操作系统可靠、数据库管理系统可靠、应用程序可靠等。

(3) 健壮性 指系统在故障情况下的恢复容易程度。

对关键硬件设备的损坏，通常采取一定程度的容错措施来应对。根据经验，系统最可能出现的故障原因依次为：电源故障，雷击，线路连接，火灾失效等。

2. 广域网的可靠性设计

广域网的可靠性包括冗余的广域网线路及其所带来的额外开销。一种主要的方法是连

接备份线路，可以避免重复路由的保持和再计算。例如，路由器通过 DDN/Frame Relay 连接主干的通信线路。当主干线路出现故障时，路由器可以自动通过 PSTN 或 ISDN 拨入中心路由。

广域网的可靠性设计包括线路的备份和中心路由器的备份。系统中以上两个部件出现故障时，系统能够自动地在数秒内切换到备份部件上，而无需人工干预。

3. 通信设备的可靠性设计

随着租用线路服务可靠性的增强及其 ISDN/PSTN 后备技术的成熟，系统的可靠性已经很大程度上转移到通信设备连接的可靠性上。

防止通信设备损坏对网络造成不良后果的较好解决方案就是使用双电源和双路供电。例如：中心路由器可以采用 Cisco 公司的高性能大型路由器 7204(Cisco7204 路由器具有双电源容错系统，并且具有端口容错等安全措施来保证系统的稳定运行)。

4. 局域网的可靠性设计

随着通信线路和通信设备的可靠性提高，系统的可靠性已经很大程度上转移到局域网连接的可靠性上。一个很好的解决方案就是使用双局域网服务。主机与两个局域网适配器相连，每个适配器连接到一个单独的集线器或交换机上，这样主机与主干交换设备之间的关键连接具有较高的可靠性。

网络设计人员应根据组网需求，选择符合要求的可靠性结构和策略。

2.1.1.10　网络高可靠性设计

什么样的网络才是高可靠的网络？

不管是网络拓扑结构的三层模型中的哪一层都应该是可靠的，这一点对于核心层网络尤其重要。核心层路由器掌握整个互联网络上所有路由器的信息，假如核心层网络瘫痪，后果将不堪设想。

可靠的核心层路由器可以通过选择新的路径，以及对于网络拓扑结构改变的迅速反应，来适应偶发的部分网段失效的情形。重新调整路由信息所耽误的时间应该很短，用户不致察觉到网络故障。

目前主流网络设备在增强系统可靠性方面做了许多工作，这些工作包括硬件可靠性和软件可靠性两个方面。以 Cisco 为例，它的 IOS 所支持的加强可靠性和随时可用性的措施包括：具有可扩充性的路由协议、路由通道和拨号备份路径。

1. 具可扩充性的路由协议

包括开放式最短路径优先(Open Shortest Path First，OSPF)、NetWare 链路服务协议(NetWare Link Services Protocol，NLSP)以及增强内部网关路由选择协议(Enhanced Interior Gateway Routing Protocol，EIGRP)。这些协议提供下列功能：

(1)　可以通达各网络

不像有些距离向量的路由协议，为了防止产生路由回路而有最大跳数的限定，OSPF、NLSP、EIGRP 等协议使用可以扩充可通达网络数的路由权值，使得网络具有可扩充性，可以连通很多的网络和子网络。

(2)　快速的收敛时间

收敛时间指的是当路由信息有变动时，将新的信息传遍整个互联网络所需的时间，当然收敛时间越短越好。路由器能很快地发现失效的网段，而且每个路由器都备有一份网络拓扑的地图，因而具有可扩充性的路由协议可以快速收敛。

(3) 阻塞控制

与吞吐量无关的带宽称为开销，例如，路由器在互相传递路由信息时所要占用的带宽就是一种开销。具有可扩充性的路由协议通过路由汇总信息，在传递更新路由选择表信息的时候，大大地降低所需占用的开销，从而减少网络阻塞的几率。

2. 替代路径

许多互联网络的骨干承担着完成企业主要任务的使命，通常企业会不计成本保护这种网络的稳固。在骨干网络上的路由器必须是稳定可靠的，不会成为整个网络中较弱的一环。要维持网络的稳固，关键在于为骨干网络提供替代路径，以备不时之需。

但是光靠提供替代路径给骨干网络并不能确保整个互联网络的端到端连接稳定可靠。例如，某区段网络中断时，该区段的信息便无法送到骨干网络上。要使得端对端的连接稳定可靠，解决方法便是在整个互联网络中添加备用路径。但是，备用路径会增加成本，所以多数企业只在重要的区段架设备用路径。

3. 负载平衡

负载平衡是在一个具有多路连接的网络上增加带宽的最简单的方法。路由器通常都具备内置的负载平衡功能，可以有多条路径通往相同的目的地，而每条路径的优先次序不一定相同。在 IP 的架构下，路由器以包种类为基础，或以包目的地为基础，提供负载平衡。

在以目的地为基础的负载平衡工作时，路由器使用路由高速缓冲存储器来决定输出的接口。当以 IGRP 或 EIGRP 为路由协议时，路由器会用路由权值来决定路径，允许不等权重的负载平衡；用户也可以手动改变权值，调整负载平衡。

由于具有可扩充性的路由协议拥有一张整个网络架构的地图，也由于这类协议维护路由选择表的方式，使它们可以同时通过不同的路径将包传送到相同的目的地。

4. 路由信道

由软件所建立的路由信道提供穿越广域网络，到另一个本来无法直接到达的网络的通信。举例来说，某公司总部和分公司都使用某种网络系统要把分公司的计算机加入总部的网络，这本来是不可能的，因为中间所经过的广域网络系统是由 TCP/IP 所架构的 Internet 系统。除非单独建立一条专线连接，或向网络服务提供商租用一条专线，中间不经 Internet 系统。但是这种做法过于昂贵，而路由信道则提供了更好的解决办法。

路由信道允许在两个不直接连接的网络之间工作的通信协议，穿越第三方网络系统建立点对点的连接，而不要求中间的第三方网络系统和两端的系统必须与该通信协议兼容。例如，连接两个 IPX 的系统，中间穿越 IP 网络，通过软件设置两端的网关，中间便可以像通过隧道一般地穿越，而不必要求中间每一转运站都能识别 IPX 包。换句话说，不论是 Netware 还是微软的网络系统，都可以通过路由信道的方法将原来的包或帧包在 IP 包里面当作 IP 包的数据，通过 TCP/IP 网络传送到终端网络，再取出原来的包用于自己的网络上。

路由信道提供了通过虚拟接口将包封装入传送协议的作业方式。这种做法不仅将原本无法通过第三者连接的网络连接起来，而且可以避免中间的各转运站为了识别不同种类的

包而启用不同的通信协议，无谓地增加额外负担。

5. 连接备份路径

在连接广域网络时，设置备份路径有如下目的：

- 通过设置一条或多条备份路径，使得网络连接更可靠。
- 当主要网络阻塞时，备份路径增加了可选的通道。

利用连接网络作为备份路径，与固定连接式的负载平衡或分散路径的做法有所不同，只在主要网络中断或阻塞时才连接备份路径，由路由器启用自动连接与自动重选路径，赋予接口新地址的功能。

2.1.1.11　确定安全性措施

不重视安全的网络是危险的，但是夸大安全威胁的防范措施也是不理智的。网络的攻击将可能带来巨大的损失，但过度的安全性措施将会严重浪费网络资源，降低网络性能，甚至会使网络产生错误结果。

网络安全的设计要用科学的方法，要对网络上的各种数据进行风险评估，然后再选择适当的网络安全机制和方法。网络安全的设计与网络应用目标密切相关。

安全性设计主要包括以下几个方面：

(1) 网络层安全　核心问题是网络能否得到控制，即是否允许任何一个客户都能进入网络。用于解决网络层安全性问题的主要方法有防火墙和虚拟专用网(VPN)。

(2) 系统安全　主要考虑的问题有两个，一是病毒对于网络的威胁；二是黑客对网络的破坏和入侵。

(3) 客户安全　对客户进行分级管理，根据不同的安全级别，将客户分成若干等级，每一等级的客户只能访问与其等级相对应的系统资源和数据，并采取强有力的身份认证措施，确保客户的密码不被他人猜测到。

(4) 应用程序的安全　涉及两方面的问题，一是应用程序对数据的合法权限；二是应用程序对客户的合法权限。

(5) 数据安全　在数据的传输过程中，对其进行加密处理，这虽然是一种比较被动的安全手段，但往往能收到最好的效果。

1. 安全性设计

安全性的设计应当在网络物理设计阶段开始前完成，以免影响物理设计。

安全性设计一般包括：

- 安全性需求分析。
- 确定确保网络安全的策略。
- 开发实现安全策略。
- 测试安全性，发现问题及时修正。

制定周期性的独立审计，阅读审计日志，响应突发事件，阅读最新的文献和代理警告，不断测试和培训，以及更新安全性计划和策略来维护网络的安全性。

网络的安全对于企业至关重要，网络的安全主要取决于采用何种安全措施，以及实现此种安全措施所使用的技术和设备，需要根据它们的实现效果做出安全评估。

2. 安全威胁

计算机网络中的通信面临以下 4 种威胁：

- 截获　攻击者从网络上窃听他人的通信内容。
- 中断　攻击者有意中断他人在网络上的通信。
- 篡改　攻击者故意篡改网络上传送的报文。
- 伪造　攻击者在网络上传送伪造信息。

截获信息的攻击称为被动攻击，而更改信息和拒绝用户使用资源的攻击称为主动攻击。

3. 总体安全解决方案

在网络的很多层都存在着潜在的弱点，因此网络安全需要分层管理，以防止数据被无意或有意地破坏。根据机构或组织的安全需求，这种总体安全解决方案的分层方法主要包括如下内容：

- 安全措施
- 用户的安全意识培训
- 物理安全措施
- 加密技术
- 访问控制
- 用户验证
- 防火墙
- Internet 协议安全(IPsec)

4. OSI 安全服务

针对网络系统受到的威胁，OSI 安全体系结构要求的安全服务内容有以下 6 个方面。

(1) 对等实体鉴别服务

对等实体鉴别服务是在两个开放系统对等层中的实体建立连接和数据传送期间，为提供连接实体身份的鉴别而规定的一种服务。这种鉴别服务可以是单向的也可以是双向的。

(2) 访问控制服务

访问控制服务可以防止未经授权的用户使用系统资源。这种服务不仅可以提供给单个用户，也可以提供给封闭的用户组中的所有用户。

(3) 数据保密服务

数据保密服务的目的是保护网络中各系统之间交换的数据，防止因数据被截获而造成的泄密。它包括以下内容：

① 连接保密　对某个连接上的所有用户数据提供保密。

② 无连接保密　对一个无连接的数据组的所有用户数据提供保密。

③ 选择字段保密　对一个协议数据单元中的用户数据的一些经选择的字段提供保密。

④ 信息流安全　防止可能通过观察信息流进行信息推导。

(4) 数据完整性服务

数据完整性服务用来防止非法实体(用户)的主动攻击(如对正在交换的数据进行修改、插入，使数据延时以及丢失数据等)，以保证数据接收方收到的信息与发送方发送的信息完

全一致。

(5) 鉴别服务

鉴别服务是某一层向上一层提供的服务，它用来确保数据是由合法实体发出的，它为上一层提供对数据源的对等实体进行鉴别。

(6) 禁止否认服务

禁止否认服务用来防止发送数据方发送数据后否认自己发送过数据，或接收方接收数据后否认自己收到过数据。

5. OSI 安全机制

为了实现上述各种 OSI 安全服务，ISO 建议了以下 8 种安全机制。

(1) 加密机制

加密是提供数据保密的最常用方法。按密钥类型划分，加密算法可分为对称密钥加密算法和非对称密钥加密算法两种；按密码体制分，加密算法可分为序列密码算法和分组密码算法两种。将加密与其他技术相结合，可以实现数据的保密性和完整性。除了会话层之外，加密均可在其他各层上进行。

(2) 数字签名机制

数字签名可解决网络通信中如下安全问题：

① 否认 发送者事后不承认自己发送过某份文件。

② 伪造 接收者伪造一份文件，声称它来自发送者。

③ 冒充 网上的某个用户冒充另一个用户接收或发送信息。

④ 篡改 接收者对收到的信息进行篡改。

(3) 访问控制机制

访问控制是按事先确定的规则决定主体对客体的访问是否合法。当主体试图非法使用客体时，该机制将拒绝这一企图，并向审计跟踪系统报告这一事件。审计跟踪系统将产生报警信息或部分追踪审计信息。

(4) 数据完整性机制

数据完整性包括两种形式：一种是数据单元的完整性；另一种是数据单元序列的完整性。保证数据单元完整性的一般方法是：发送实体在一个数据单元上加一个标记，这个标记是数据本身的函数(如分组校验或密码校验函数)，它本身是经过加密的。接收实体接收到一个对应的标记，并将所产生的标记与接收的标记相比较，以确定在传输过程中数据是否被修改过。

数据单元序列的完整性要求数据单元序列具有数据编号的连续性和时间标记的正确性，以防止假冒、丢失、重发、插入或修改数据。

(5) 交换鉴别机制

交换鉴别是以交换信息的方式来确认实体身份的机制。用于交换鉴别的技术有以下两种：

① 口令 由发送方实体提供，接收方实体检测。

② 密码技术 将交换的数据加密，只有合法用户才能解密，得到有意义的明文。在许多情况下，这种技术与下列技术一起使用：

- 时间标记和同步时钟

- 双方或三方“握手”
- 数字签名和公证机构
- 利用实体的特征或所有权

(6) 业务流量填充机制

业务流量填充机制主要防范非法者在线路上监听数据，并对其进行流量和流向分析。采用的方法一般由保密装置在无信息传输时，连续发出伪随机序列，使得非法者不知哪些是有用信息，哪些是无用信息。

(7) 路由控制机制

在一个大型网络中，从源节点到目的节点可能有多条通路，有些可能安全，有些可能不安全。路由控制机制可使信息发送者选择路由，从而保证数据安全。

(8) 公证机制

在大型网络中，需要有一个各方都信任的实体——公证机构来提供公证服务。通信双方进行数据通信时必须经过公证机构转换，以确保公证机构得到必要信息，供以后仲裁时使用。

6. 网络信息安全系统的设计原则

在网络信息安全设计之初，应当遵循一些合理的原则，使相应网络信息系统的安全和保密更加有保障。从工程技术角度出发，在设计网络信息系统时，至少应该遵守以下设计原则：

(1) “木桶”原则

攻击者使用的是“最易渗透原则”，必然在系统中最薄弱的地方进行攻击。因此，充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测(包括模拟攻击)，是设计信息安全系统的必要前提条件。安全机制和安全服务设计的首要目的是防止最常用的攻击手段，根本目标是提高整个系统的“安全最低点”的安全性能。

(2) 整体性原则

信息安全系统应该包括三种机制：安全防护机制、安全监测机制和安全恢复机制。安全防护机制是根据具体系统存在的各种安全漏洞和安全威胁采取相应的防护措施，避免非法攻击；安全监测机制是监测系统的运行情况，及时发现和制止对系统进行的各种攻击；安全恢复机制是在安全防护机制失效的情况下，进行应急处理，减少攻击的破坏程度。

网络信息安全系统的整体性原则就是统一实现安全防护、监测和应急恢复。

(3) 有效性与实用性原则

网络中的信息安全和信息共享之间存在着一个矛盾：一方面，为健全和弥补系统缺陷的漏洞，会采取多种技术手段和管理措施；另一方面，过多的技术手段和管理措施势必给系统的运行和用户的使用造成负担和麻烦，尤其在网络环境下，实时性要求很高的业务难以容忍安全连接和安全处理造成的时延和数据扩张。

如何在确保安全性的基础上，把安全处理的运算量减小或分摊，减少用户记忆、存储的工作量和安全服务器的存储量、计算量，这是需要信息安全设计者应该着力解决的问题。

信息安全系统的有效性与实用性原则是不应该影响系统的正常运行和合法用户的操作活动。

(4) 安全性评价原则

实用安全性与用户需求和应用环境紧密相关。因此，评价信息安全系统是否安全，没有绝对的评判标准和衡量指标，只能取决于系统的用户需求和具体的应用环境。

信息安全系统的安全性评价原则是实用安全性与用户需求和应用环境紧密相关。

(5) 等级性原则

良好的信息安全系统必然分为不同级别，包括：对信息保密程度分级(绝密、机密、秘密、普密)，对用户操作权限分级(面向个人及面向群组)，对网络安全程度分级(安全子网和安全区域)，对系统实现结构的分级(应用层、网络层、链路层等)。针对不同级别的安全对象，提供全面的、可选的安全算法和安全体制，以满足网络中的实际需求。

信息安全系统的等级性原则就是通过设置安全层次和安全级别来保证系统的安全性。

(6) 动态化原则

被加密信息的生存期越短，可变因素越多，系统的安全性能就越高，例如，周期性的更换口令和主密钥，安全传输采用一次性的会话密钥，动态选择和使用加密算法等。

信息安全系统的动态化原则是整个系统内尽可能引入更多的可变因素，并使其具有良好的扩展性。

(7) 设计为本原则

在网络进行总体设计时就应考虑安全系统的设计，将两者合二为一。设计为本原则就是安全与保密系统的设计应与网络设计相结合。

(8) 权限分割、互相制约、最小化原则

在很多系统中都有一个系统超级用户或系统管理员，拥有对系统全部资源的存取和分配权，因此有必要对系统超级用户的权限加以限制，实行权限最小化原则，并实现管理权限交叉，即有几个管理用户来动态地控制系统的管理，实现互相制约。而对于非管理用户即普通用户，同样实行权限最小原则，不允许其进行非授权的操作。

(9) 有的放矢、各取所需原则

实际上网络系统的设计是受经费限制的，因此在考虑安全问题解决方案时必须考虑性能和价格的平衡。不同的网络系统所要求的安全侧重点各不相同，例如，国家政府首脑机关、国防部门计算机网络系统安全侧重于存取控制强度；金融部门侧重于身份认证、审计、网络容错等功能；交通、民航侧重于网络容错等。所以必须有的放矢，具体问题具体分析。

2.1.1.12 网络设备的选择

网络设备质量高低直接影响到网络系统的性能。选择设备时，首先必须制定选择标准，即根据用户单位实际需要制订成本、性能、容量、处理量、延迟等指标和浮动范围，在能够满足需求的情况下，没有必要一味求高求贵，而要参照产品的性能价格比来决定。

在设备到达现场时，需要检验其标称性能参数与既定标准的一致性，看是否有性能不达标的产品存在，以免一旦投入运行后影响整个系统的性能。

设备安装到位初步调试通过后，还需要采取专门的测试手段对关键设备进行高级测试，考查设备在实际环境中的性能表现和与其他设备的兼容性和互联性能完全符合标准后才能通过验收。

在选择产品时，除了要求产品支持应用需求之外，还建议考虑如下因素：选用符合工

业标准的流行产品(保证产品的兼容性、可靠性和可扩充性)，具有较多的工具软件和应用软件支持，具有进一步开发的接口，具有完整的资料说明等。

作为网络工程，被选择的产品主要包括传输介质、网络接口、互联部件、网络服务器以及网络通信协议和应用软件等。

1. 传输介质

传输介质是网络的最基本部分，用于在用户设备之间传输信号。选择传输介质时，应当考虑如下因素：

- 安装特性　包括单段介质的最大长度、网络的覆盖范围、铺设时允许的最小弯角和最大直径等。
- 连接性　包括网络拓扑、可支持的连接数据等。
- 容量及性能　包括可使用的带宽、支持的逻辑信道数、每个信道可以支持的最大传输速率等。
- 防护性能　包括电气干扰与噪声、物理损害、安全性等。
- 价格　介质的价格。

目前可以选择的介质类型包括如下几类：

- 无屏蔽双绞线　支持点到点连接(包括环形)，价格较低，用于计算机联网的双绞线应为三类线以上。
- 屏蔽双绞线　支持点到点连接(包括环形)，仅用于电磁干扰较严重的环境，价格适中。
- 基带同轴电缆　支持总线连接(包括环形)，价格适中。
- 宽带同轴电缆　支持总线连接(包括环形)，价格略高。
- 光纤　支持点到点连接(包括环形)，价格偏高。

随着结构化布线技术的推广，以及多介质应用的增多，双绞线和光纤成为组网的主要传输介质。

需要指出的是，传输介质的选择应当具有足够的超前意识，因为传输介质的布放一般会对建筑物的本身造成影响，因此应当尽可能减少因设备的更新换代和升级而改变传输介质。

2. 网络接口

网络接口的用途是将用户设备接入网络，通常以网络适配卡的形式出现。使用不同的传输介质和采用不同的访问介质控制方法要求不同类型的网络适配卡。

目前，常用的网络适配卡包括：

- 以太网卡　支持总线方式，具有不同的速率和工作方式的接口，可以连接双绞线、同轴电缆和光纤。
- ARCnet 网卡　支持总线方式，具有不同的接口，可以连接双绞线、同轴电缆，常用于生产控制环境。
- 令牌环卡　支持环形结构，连接双绞线。
- X.25 卡　支持用户终端接入 X.25 网络，连接双绞线。
- ATM 适配卡　支持用户设备接入 ATM 网络，连接光纤。

- FDDI 适配卡　支持用户设备接入 FDDI 网络，连接光纤或者铜芯电缆。

3. 互联部件

互联部件主要用于网络的扩展或者网络的互联。为了结构化布线的需要、减少设备之间的干扰和方便系统升级，局域网组建建议采用集线器方式。常用的互联部件包括：

- 集线器　具有一般集线器和智能集线器之分，主要用于连接节点，所有端口共享链路带宽。
- 交换器(交换式集线器)　一种采用线路交换技术的集线器，具有端口链路分隔的特征，常用于连接网段或者相同类型的局域网。
- ATM 交换机　可以直接连接节点，或者和其他 ATM 交换机连接，形成 ATM 网络。
- FDDI 集中器　可以直接连接节点，或者和其他 FDDI 集中器等连接，形成 FDDI 网络。
- 路由器　常用的路由器包括远程访问路由器(支持远程用户通过拨号/专线方式访问内部网)、局域网/广域网路由器(支持用户通过各种公共网络进行互相访问)。

目前较高档的互联部件均采用了模块化结构，允许用户根据具体的应用需求选择和插入不同的模块。

当选用交换器或者交换机时，应当注意其内部的交换结构；选用路由器时应当考虑采用的路由算法，以及支持分组过滤的安全策略。

4. 网络服务器

网络服务器通常是小型机或者高档微机，通过网络适配卡接入网络，向用户提供各种共享服务，例如：文件共享、打印共享、通信共享、电子邮件和 WWW 服务等。网络服务器可根据服务的类型，扩充不同的设施，例如：文件服务器要求较大容量的硬盘和高速缓冲区支持，打印服务器应当配置打印机。原理上，一台服务器可以提供多种应用服务，但在实际应用中，尤其是从安全和可扩展的角度出发，仍然建议在经费许可的前提下，根据应用服务划分和配置多台服务器。

5. 通信协议和应用软件

通信协议和应用软件的选择除了要满足具体的应用需求之外，还应考虑开放性，不仅要保证和不同厂家的不同产品之间的相互操作，还应兼顾和其他相关部门之间的关系(例如：对于数据库管理系统的选择应当兼顾与上级部门选择的一致性)。设计时应当允许三个阶段的并存，即原有的网络协议软件可能是“封闭”的，仅适合于连接同一厂家的产品(大多数生产控制系统具有这样的特性)；现行的网络协议软件要求是“开放”的，此时的整个网络系统为“混合型”的；将来的系统是完全“开放”的。

需要指出的是，任何一个系统(包括网络系统)都具有一定的生命周期，因此，应当从系统的功能、技术和效益等方面，对所设计的系统做出正确的系统生命期估计。就现阶段而言，TCP/IP 协议应是通信协议选择的主流。

产品选择阶段的工作应由专业技术人员完成，或者直接委托供应商和公司完成。当采用委托方式时，应在企业代表的全面控制下进行。

在选择供应商时，建议考虑如下因素：资金相对雄厚且具有良好业绩，可以提供可靠的产品，可以提供可靠的服务质量，尤其是售后服务质量好的公司。组建网络的最终目的

是应用，因此，具有相关拳头产品，或者应用软件开发能力也可成为选择供应商的指标之一。

2.1.1.13 设计管理

网络设计方案管理任务包括设计复查、设计验证、设计确认和设计变更。

(1) 设计复查 项目计划中规定，对设计结果必须复查且对复查应留有备案。

(2) 设计验证 在项目计划中，经过设计复查和测试后，设计验证才完成。按照复查结果验证设计输出是否符合设计输入需求，如果任一部分的设计未通过验证，必须进行设计修复。

(3) 设计确认 设计确认就是确保产品遵照产品需求说明书设计。

产品的质量保证依赖于用来进行验证、确认和控制的测试工具，以及在确认及验证阶段使用的程序。

(4) 设计变更 设计变更需要修改相关设计文档并备案。

2.1.1.14 新网络业务运营计划

新网络运营过程一般是公司业务由旧的网络向新的网络迁移的过程。旧有业务应用适合于原有网络，而新系统由于在功能、性能、技术等方面都与旧有网络系统存在较大差异，因而对业务系统的支持也不同，直接将旧有业务系统迁移到新系统上是不太现实的，新系统的使用往往与新的业务系统配套。

在向新系统升迁前，应该周密计划，需要仔细考查新、旧系统的差异，分析升迁对用户造成的影响并及时通知他们，考虑到用户不能很快接受并适应新系统，升迁前还需要对他们进行系统的业务操作培训。如果一个单位的业务应用分为若干部分，也可以按照先易后难的顺序，一个部分一个部分地迁移到新系统，逐步积累新系统的使用经验，为后续部分的升迁做准备。

在整个升迁过程中，要及时做好系统备份，包括旧系统的备份，以便在新系统不可用时能够及时恢复到旧有系统，保证业务正常开展。迁移完毕后，还需要对新业务系统进行测试，检查其对于设计目标的可满足性。当新系统迁移成功后，对旧系统应采取措施妥善处理。

所有这些工作都将在网络系统实施阶段完成，因而在设计阶段应该针对每一个环节制定详细的计划，以便以后按计划实施。

2.1.1.15 设计方案测试

测试一个网络、预测和衡量网络性能是一门科学。没有两个完全相同的系统，因此对测试方法和测试工具的正确选择需要具有一定的创造性，还需要对所测试的系统有透彻的理解，这就需要用测试手段来加以鉴别和测试网络设计方案的正确性。

1. 测试原型网络系统

根据所要测试的项目的目的决定正确选择测试方法和测试工具，通常包括以下内容：

- 验证该设计是否满足商业技术目标。
- 验证所选择的局域网技术、广域网技术和设备是否合适。

- 验证服务提供者是否能够提供要求的服务。
- 找出系统瓶颈或连通性问题。
- 测试网络冗余。
- 分析网络链路故障对性能的影响。
- 确定必要的优化技术，满足性能和其他技术目标。
- 分析网络链路和设备升级对性能的影响。
- 证明该设计优于其他竞争方案。
- 通过一个“验收测试”获得进行下一步的网络实现。
- 发现可能妨碍执行的风险，并拟定相应的补救措施。
- 决定还需要多少其他测试。

如果网络设计方案中选用的设备不是全新的设备，也即该设备或相应的组网方案已经得到应用，上述测试内容就可以大大简化。一个比较简单的方法是，考察采用类似方案的现有网络系统，如果可能，可以考虑在不影响该网络的业务正常运行的前提下，支付必要的费用，对该网络进行所需要的测试。这种方法的优点是，可以节省大量的资金和时间，与实际结合比较紧密。

如果采用的是全新的设备和网络设计方案，也应该要求设备厂商进行必要的测试或提供尽可能全面的测试资料，特别是第三方的权威测试结果报告，以降低测试费用。

2. 建立和测试原型网络系统

原型网络系统是新系统的一个初始实现，为最终完成系统提供了一个样板，帮助网络设计者验证所设计的新系统的功能和性能。

建立和测试原型网络系统能否顺利实施取决于所能得到的资源支持，包括人工、设备、资金和时间等。完成有效的测试需要有足够的资源，但是如果资源消耗过高会导致项目预算超支、时间过长或对用户产生不利影响。

以下就是建立和测试原型系统常用的 3 种方法：

- 在实验室中建立和测试网络。
- 与正在运行的网络集成，利用空闲时间进行测试。
- 与正在运行的网络集成，在正常工作时间内测试。

一旦网络设计方案得到认可，剩下的关键问题就是对原型网络系统进行测试，以考察可能出现的设计瓶颈。这种测试可以在空闲的时间进行，但最终的测试必须放在正常的工作时间内进行，从而能够在正常负载的情况下对系统进行评估。

在确定了原型系统的测试范围后，应该制定测试计划，说明如何测试该原型系统。

测试计划设计的内容应当包括以下方面：

- 测试目标和验收标准。
- 测试的种类。
- 网络设备和所需的其他资源。
- 测试脚本。
- 测试项目的时间划分和阶段划分。

测试计划执行的过程主要是按测试脚本执行并将工作归档。由于在编写测试脚本时不可能把所有突发情况和可能出现的各种问题都考虑到，故无法按部就班地执行测试计划。

所以，在测试计划执行的过程中对日志记录进行维护就显得非常重要。

日志记录应当包括测试数据和测试结果以及每日活动记录。每日活动记录用来记载测试记录，包括对测试脚本或设备配置所做的改变，遇到的问题和对引起这些问题原因的推测。这些推测记录在分析测试结果中往往能够发挥重要的作用。

3. 网络测试工具

一般网络设计的测试工具包括：

- 网络管理和监控工具。
- 建模和仿真工具。
- 服务质量和服务级别管理工具。

2.1.1.16 设计评审

对于按照以上规范提出的网络逻辑设计方案，必须得到批准后才能够实施。

先交由单位组建的网络评审委员会讨论，审查该方案是否满足本单位对新网络的各种类型的需求，网络规划是否合理，使用的技术是否先进，采取的设备厂商是否信誉良好，网络的实施成本是否在单位的预算之内等，不同的单位可能有不同的审查准则。在所有条件均满足之后，网络设计方案才得到批准。

批准时，需要由单位的管理部门、MIS 职员和咨询公司代表签字。

2.1.2 典型例题分析

例 1 在网络规划阶段“系统可行性分析和论证”的主要内容是什么(控制在 100 个字以内)？(2001 年下午试题二问题 2)

分析：可行性分析是结合用户单位的具体情况，论证建网目标的科学性和正确性。通过可行性分析可以提出一个解决用户问题的网络体系结构，它包括以下 4 方面内容：

(1) 传输 传输方式用基带还是宽带传输，通信类型及通道数，通信容量，数据传输速度。

(2) 用户接口 支持的协议，工作站类型，主机类型。

(3) 服务器 类型，容量，协议。

(4) 网络管理能力 网络管理，网络控制，网络安全。

对于网络体系结构的描述，在可行性论证阶段应尽可能用与厂家无关的功能术语。

系统可行性的一个重要影响因素是造价，而这一部分是要进行方案设计之后才能确定的。网络系统的方案往往不止一个，而且实施的效果和可靠性保证也不尽相同，用户的决策者可以从中选择出最佳方案。

答案：

可行性分析主要是针对用户单位具体情况，对建网的目标进行科学性和正确性论证。在此基础上提出一个解决用户问题的网络体系结构。包括网络传输、用户接口、服务器和网络管理，以及对投资及建设周期的估算。

例 2 阅读以下说明，回答问题 1 和问题 2，将解答填入答题纸的对应栏内。(2003 年下午试题一)

【说明】

某学校拟组建一个小型校园网，具体设计如下：

(1) 设计要求

① 终端用户包括：48 个校园网普通用户；一个有 24 个多媒体用户的电子阅览室；一个有 48 个用户的多媒体教室(性能要求高于电子阅览室)。

② 服务器提供 Web、DNS、E-mail 服务。

③ 支持远程教学，可以接入互联网，具有广域网访问的安全机制和网络管理功能。

④ 各楼之间的距离为 500m。

(2) 可选设备如表 2.1 所列。

表 2.1　小型校园网要求

设备名称	数　量	特　性
交换机 Switch1	1 台	具有两个 100Base-TX 端口和 24 个 10Base-T 端口
交换机 Switch2	2 台	各具有两个 100M 快速以太网端口(其中一个 100Base-TX、一个 100Base-FX)和 24 个 10Base-T 端口
交换机 Switch3	2 台	各配置 2 端口 100Base-FX 模块、24 个 100Base-TX 快速以太网端口
交换机 Switch4	1 台	配置 4 端口 100Base-FX 模块、24 个 100Base-TX 快速以太网端口；具有 MIB 管理模块
路由器 Router1	1 台	提供了对内的 10M/100M 局域网接口，对外的 128K 的 ISDN 或专线连接，同时具有防火墙功能

(3) 可选介质：3 类双绞线、5 类双绞线、多模光纤。

该校网络设计方案如图 2.4 所示。

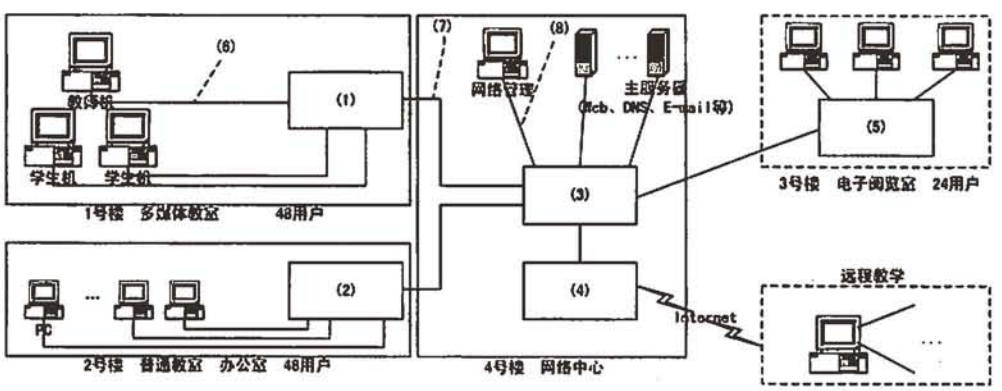


图 2.4　某学校的网络设计方案

【问题】

1. 依据给出的可选设备进行选型，将(1)~(5)处空缺的设备名称填写在答题纸相应位置(每处可选一台或多台设备)。

2. 将(6)~(8)处空缺的介质填写在答题纸相应位置(所给介质可重复选择)。

分析：交换机和路由器都是网络中继设备，交换机工作在 OSI 数据链路层，用于互联

两个独立的同类子网，实现信息帧的存储-转发。路由器工作在网络层，用于互联两个不同类型的子网。由图中网络结构不难确定(1)~(5)中的设备。

双绞线是局域网中最常用的传输介质，EIA/TIA 定义了 7 种规格，常见的有三类和五类，它们分别提供 16Mb/s 和 100Mb/s 的带宽，除了带宽上有差别外，由于使用特殊工艺五类双绞线还在抗干扰能力和衰减特性方面大大优于三类线。但是双绞线在连接跨度上有限制，一般在 100m 左右，而各楼间相隔 500m，使用多模光纤是最佳选择。光纤传输速率快，传输距离可达 2km，信号无失真、误码率低、绝缘性能好、抗干扰能力强、体积小、重量轻，是结构化综合布线建筑群子系统首选媒体。

答案：

1. (1) 两台交换机 Switch3
   (2) 一台交换机 Switch1 和一台交换机 Switch2
   (3) 一台交换机 Switch4
   (4) 一台路由器 Router1
   (5) 一台交换机 Switch2
2. (6) 五类双绞线
   (7) 多模光纤
   (8) 五类双绞线

例 3 阅读以下说明，回答问题，将解答填入答题纸的对应栏内。(2003 年下午试题二)

【说明】

在一幢 11 层的大楼内组建一个局域网，该局域网的连接示意图如图 2.5 所示。

【问题】

1. 指出上述解决方案存在什么问题？需要增加什么设备？如何连接？
2. 若在该局域网实现虚拟网，路由器将起什么作用？

分析：路由器工作在 OSI 第三层，用于连接不同的网络，转换不同的网络协议分组。路由器的功能需要由内置软件来实现，因此性能方面不如依靠硬件实现的交换机。按照图中连接方法，势必影响各楼层客户端 PC 机访问服务器的效率，况且整个智能大厦中是同种网络，内部访问无需路由，所以增加一个主干交换机是必需的，它用于连接各层楼内的交换机，在楼层与楼层、楼层与服务器间交换数据，提高了系统的性能。内部用户访问外网时才需要通过路由器。

虚拟网代表一个广播域，需要由交换机或路由器实现内部和外部转发功能。

答案：

1. (1) 这种方案存在的问题：缺少主交换设备。

(2) 解决方法是增加一台主交换机。

(3) 连接的方法为：各楼层交换机分别连接到主交换机，服务器均连接到主交换机，主交换机连接到路由器，如图 2.6 所示。

2. 路由器的作用就是在各个虚拟网之间进行数据转发。

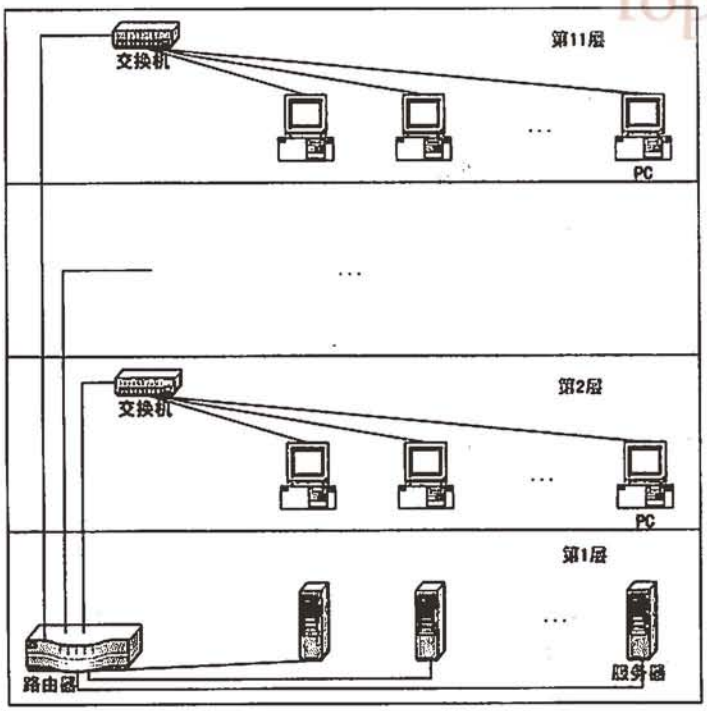


图 2.5 某局域网的连接示意图

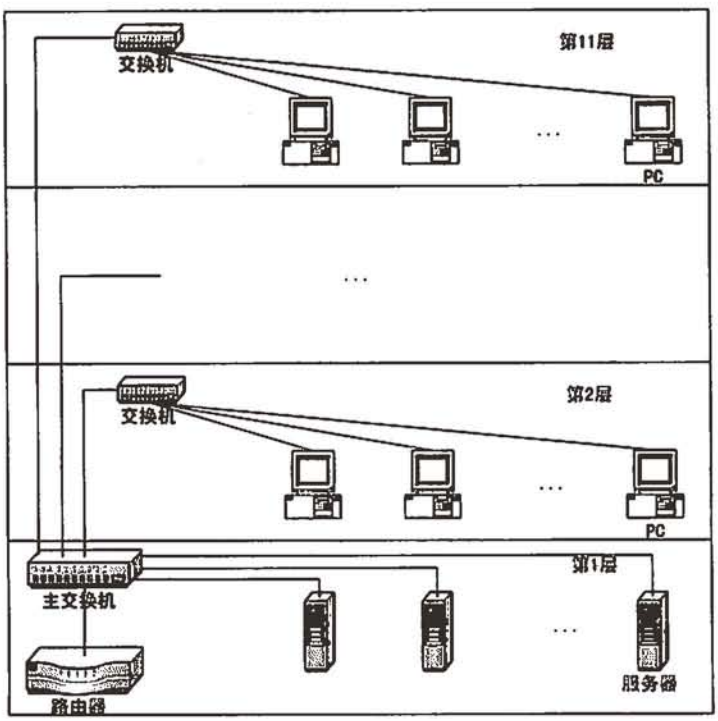


图 2.6 连接方法示意图

2.1.3 同步练习

1. 什么是可扩展的网络？它有哪些特点？
2. 三层式层级模型中各层的主要特点是什么？
3. 计算机局域网是由哪些部件组成的？

2.1.4 同步练习参考答案

1. 可扩展的网络一般是指面对持续增长的网络具有扩展性，不需要作重大修改的网络架构。它的主要特点有：稳定可靠、随时可用、反应敏捷、效率高、适应能力强以及安全性好等。

2. 典型的三层式层级模型包括核心层、分布层和接入层。

(1) 核心层追求的是最高的有效带宽，不做网络控管或包筛选的工作。

(2) 分布层连接核心层与接入层，过滤包，控管流量，某些大型服务器设置于此层内。

(3) 接入层直接对用户提供服务，工作组和大部分的应用服务器存在于此层之中。

3. 计算机局域网一般由通信传输介质、网卡、网络主干通信设备、网络服务器、联网计算机和网络操作系统组成。

2.2 本 章 小 结

网络设计是构建网络系统的第二个阶段，也是非常重要的一个阶段。本阶段的任务是根据用户建网需求，来选择建网所使用的技术、产品设备、拓扑结构，并确定网络性能、可靠性、安全性等指标，提出详尽的、完善的、合格的网络系统设计方案，作为下一步网络系统施工的依据。本章着重介绍了在网络系统设计阶段应该考虑的关键问题和应采取的措施。

第 3 章　网络系统的构建和测试

大纲要求：

- 安装工作　事先准备，过程监督。
- 测试和评估　连接测试，安全性测试，性能测试。
- 转换到新网络的工作计划。

3.1　网络系统的构建和测试

3.1.1　考点辅导

3.1.1.1　安装工作

1. 网络实施过程

网络实施是在网络设计的基础上，进行设备的购买、安装、调试、培训和系统切换等工作。网络实施包括以下步骤：

(1) 工程实施计划

在网络安装前，需要准备一个工程实施计划，列出需安装的项目、安装费用、安装负责人等，以便控制投资和进度，按进度要求完成安装任务。工程计划必须包括网络实施阶段的设备验收、人员培训、系统测试以及网络运行维护等具体事务的处理，必须合理安排工程实施的时间，并充分调动有关人员的积极性。

(2) 网络设备到货验收

订购的网络设备到货后，在安装调试之前，必须先进行严格的功能和性能测试，以保证购买的产品能很好地满足用户需要。

(3) 设备安装

网络系统的工程安装和调试要由专门的技术人员负责。安装项目一般可分为：布线系统、网络设备、主机服务器、系统软件、应用软件等几个部分，不同部分应由专门的工程师进行安装调试。

(4) 系统测试

系统安装完毕，要进行系统测试。系统测试是保证网络安全可靠运行的基础。

(5) 系统试运行

系统调试完毕，进入试运行阶段。这一阶段的任务主要是验证系统在功能上、性能上是否达到预期目标，如不满足则需要不断调整直至达到用户要求。

(6) 系统切换

系统经过一段时间的试运行，达到稳定可靠的水平，就可以进行系统切换了。系统切换是指从原有人工或计算机系统上迁移到新平台上工作，有三种切换方法：双运行方式(两

种方式同时运行)、逐步替代法(新系统逐步替代原有的网络系统)和直接切换法(停止旧系统，启动新系统)，显然这三种方法的可靠性和成本各不相同，应视具体情况而定。

(7) 人员培训

对有关人员的培训是网络建设的重要一环，也是保证业务正常开展的一个重要因素。一个规模大、结构复杂的网络系统往往需要网络管理员来维护网络，协调网络资源的使用。

2. 结构化综合布线系统

结构化综合布线系统是一种模块化、灵活性极高的建筑物和建筑群内的信息传输系统。结构化综合布线系统(SCS)是一种集成化的通用传输系统，它利用双绞线或光缆来传输建筑物内的多种信息。

在现代化的大型建筑中，除计算机网络系统以外，通常还会有电话系统、楼宇控制系统等各专业布线系统。传统的做法是，为不同的专业系统配置不同的线缆、插座及接头等不同的布线材料来构成各自网络；连接这些不同网络的插头、插座及配线架互不兼容，只要变动终端机的位置，就必须重新布放新的线缆，安装新的插座。在这种传统的布线方式下，因办公室的重新规划及办公设备的变更而导致布线系统的变更要耗费大量的金钱和时间，同时，对于布线系统的日常维护和管理、故障的检查和排除都不太方便。

为解决传统布线方式中的种种弊端，工业界推出了结构化综合布线系统。SCS 将所有的语音、数据、图像及监控设备的布线组合在一套标准的布线系统上，采用统一的线缆、插头、插座及配线架，当终端机的位置需要变动时，只需将其插入新地点的插座上，然后作一些简单的跳线即可，不需要再布放新的线缆，也不需要安装新的插孔。另一方面，SCS 采用星形结构，系统的管理维护及故障的检查和排除也非常方便。SCS 以其高度的灵活性及多元化服务而越来越得到人们的重视。

SCS 可以划分为 6 个子系统：

- 工作区子系统(用户端子)
- 水平布线子系统
- 干线子系统
- 设备间子系统
- 管理子系统
- 建筑群子系统

(1) 工作区子系统

工作区子系统是结构化综合布线系统中将用户的终端设备连接到布线系统的子系统。工作区子系统包括各种不同型号的信息插座、适配器、连接跳线等将设备连到插座上所需的各种配件。

工作区是一个独立的需要设置终端设备的区域，它的服务面积一般按 $5m^2$~$10m^2$ 估算，每个工作区设置一个电话插座和一个计算机插座，信息插座是终端设备与水平子系统连接的接口，8 针模块化信息插座是为所有的综合布线系统推荐的标准 I/O 插座。

信息插座的数量一般由使用者的数量所决定，如果使用者的数量不能确定，有一些经验值可供参考。根据经验在办公环境下一般可考虑 $9m^2$ 设置一个工作区，安装一对信息插座(一个接电话、一个接计算机)。但这仅是一个参考，在具体设计和施工过程中，设计单位和用户单位应根据具体情况灵活掌握。

(2) 水平布线子系统

水平布线子系统是结构化综合布线系统中连接用户工作区与布线系统主干的子系统。水平子系统由每层配线间至信息插座的配线电缆和工作区用的信息插座等组成。在结构化综合布线系统中，水平布线子系统起着支线的作用，它将所有用户端通过一些连接件连接到配线设备上。

水平布线方式受到很多因素的影响，常用的布线方式大致有两种：一种是直接铺设管线方式，它采用星状结构，利用金属线槽或金属管从布线系统的干线接线间或卫星接线间直接引到每个信息点；另一种是线槽管道布线法，通常是在天花板内安装线槽，再用管线从线槽引到每个插座。

在新建建筑中，布线系统的设计应在设计大楼的图纸时考虑，并融进大楼的弱电图中，以便在施工过程中暗铺相关的线槽和管线，预留墙面出口，安装插座底盒。

(3) 干线子系统

干线子系统是结构化综合布线系统中连接各管理间、设备间的子系统，又称垂直子系统。干线子系统是综合布线系统的骨干，包括：

- 供干线电缆走线用的垂直或水平通道
- 设备间与网络接口之间的连接电缆
- 设备间与建筑群子系统之间的连接电缆
- 干线接线间与各卫星接线间之间的连接电缆
- 主设备间与计算机中心之间的电缆

综合布线系统的干线可根据距离的远近和用户对传输速率及传输质量的要求，选择多对数双绞线或光缆。一般在楼内的语音通信采用三类的大对数双绞线作为主干；数据通信可以采用高品质的五类双绞线，也可以采用光缆；如果电磁干扰严重，则推荐采用光缆作为数据主干。在做干线子系统的设计时，首先要确定每一层楼干线需求，总结出整座楼的干线总体需求，确定干线电缆的种类及大小尺寸，然后确定干线电缆路由通道。

干线的路由通道有两大类，即封闭型和开放型。开放型通道通常是指从建筑物的地址集中安装大型通信设备的场所，如 PABX、大型计算机、计算机网络通信中枢等。

(4) 设备间子系统

设备间子系统主要用来安放网络关键设备，地位十分重要。并非每一个综合布线系统都有设备间子系统，但在大型建筑物中一般是有的，而且有时还不止一个。设备间子系统中的电话、数据、计算机主机设备及其保安配线设备宜设在一个房内。必要时，也可以分别设置，但程控交换机及计算机主机房距离设备间不宜太远。设备间的位置及大小应根据设备的数量、规模、最佳网络中心等内容综合考虑确定。在设备间子系统的设计和安装过程中还需要综合考虑配电系统(不间断电源 UPS)和安全因素(设备接地等)。

(5) 管理子系统

管理子系统是结构化综合布线系统中对布线电缆进行端接及配线管理的子系统。

管理子系统通常设置在一幢大楼的中央设备机房和各个楼层的配线间。一般由配线架和相应的跳线组成。通过管理子系统，用户可以在配线架上灵活地更改、增加、转换、扩展线路，而不需要专门工具或专业技术人员。正是通过这些功能，结构化综合布线系统才具有传统布线无法比拟的开放性、扩展性和灵活性。

(6) 建筑群子系统

建筑群子系统是结构化综合布线系统中由连接楼群之间的通信传输介质及各种支持设备组成的子系统。建筑群子系统也称为户外子系统，其传输介质除了各种有线手段之外，还可包含其他无线通信手段，如微波、无线电通信等。

户外电缆在进入大楼时通常在入口处经过一次转接接入户内系统，在转接处可以加上电器保护设备。现代化电话通信系统中通信线路在进入楼群时一般都考虑这一点，主要是避免因雷击或与高压线接触而给人和设备安全带来的损失。建筑群子系统布线方式有以下几种：地下管道敷设方式、直埋沟内敷设方式、架空等，不同方式各有优缺点。

(7) 相关标准

结构化综合布线方面的标准有 EIA/TIA 568A 和 EN 50173，分别是北美和欧洲标准，它们都规定利用铜介质双绞线的特性实现数据链路的平衡传输，只在抗电磁干扰要求方面有差异。ISO/IEC 11801 是 1995 年由 ISO 确定的国际标准。我国相关规范如下：

- GB/T 50311—2000 《建筑与建筑群综合布线系统工程设计规范》
- GB/T 50312—2000 《建筑与建筑群综合布线系统工程验收规范》
- GB 2887—89 《计算站场地技术条件》
- GB 50174—93 《电子计算机机房设计规范》
- GB 9361—88 《计算站场地安全要求》

3. 网络主干设备安装调试

在网络布线工程完工且验收合格后，一旦选配的局域网主干设备到货，就进入了网络主干构建阶段。构建从设备安装调试开始，通常由设备供应商派出的技术人员进行。网络管理员的任务是在参加设备安装调试工作的同时尽快熟悉系统构建的操作，并且把好安装调试质量关。

网络主干交换设备安装调试的步骤通常如下：

(1) 拆箱检验

与设备供应商共同打开硬件设备的包装箱，确认其中的设备符合订购要求，确认包装中的内容与装箱单一致，确认设备在运输过程中没有受损，确认所配置的软件、说明书和附件齐备。

(2) 设备安装

网络主干使用的交换机通常都是机架式设备，配备带有风扇的专门机柜。将交换机通过支架安装固定在机柜内。确认电源插座的电压和设备卡上规定的电压相符合，连接设备电源。

(3) 连接网络线缆

交换机上常见的双绞线通信端口有两种：一种是供直接连接用户设备的直通电缆端口；另一种是供与其他交换机连接的级联端口，线缆用的都是 RJ-45 插头，安装时需要注意看说明书。

配备千兆以太网的光纤接口交换机，需要使用不同的千兆以太网接口转换器 GBIC，分别提供对 100Base-LX、1000Base-SX 和 1000Base-LH 等单模光纤和多模光纤使用长波/短波激光信号传输的支持。GBIC 使用 SC 类型的光缆插头，光缆另一端使用的插头类型要与所连接的设备匹配。注意使用光纤跳线时，要与 GBIC 支持的光纤类型匹配。最后根据

网络设计方案将交换机网络线缆连接好。

(4) 连接交换机控制台设备

交换机通常都提供一个串行接口，网络管理员可以通过该接口连接计算机终端设备，监控、配置、调试和管理交换机。通常技术人员通过交换机配件中提供的转换线缆，将一台笔记本电脑或台式计算机连接到交换机上标识为控制台的串行口，在用作控制台的计算机上启动终端仿真程序。这种管理方式的优点在于无论交换机是否与网络连通，都可以通过计算机进行配置管理操作。

(5) 加电调试

在上述准备工作完成后，可以打开交换机电源开关，观察加电自检。通常加电后交换机所有端口的指示灯都闪亮，然后按照设备内置的程序进行硬件检测。在检测时各种指示灯会不断变化状态，报告检测进展情况。同时在控制台计算机屏幕上有文字显示。设备加电自检后显示的具体内容随设备不同而各异，需要仔细阅读说明书。如果一切与说明书所示的情况一样，则表示加电自检通过。

(6) 主干设备参数配置

在完成了局域网主干设备的安装调试，设备自检正常，网络线缆连接完毕后，就进入了网络主干设备参数配置阶段。对于一个仅用于小型办公室环境的简单局域网来说，如果数据通信仅限于第 2 层交换，接入层交换机又没有需要上连的主干交换机，设备提供的默认参数往往就可以满足联网要求，将入网设备连接到交换机的端口后，局域网就可以立即开始工作了。

但是对于一个具有多个层次且结构复杂的局域网而言，必须在完成对所有构成网络主干的交换机的系统参数配置后，局域网才能够正常工作。

通常在进行网络主干设备配置前，应该制定一个计划，并且将计划以文档形式确认下来，画出网络布局示意图。在计划中，应该对各个设备的名称、访问密码、设备地址、设备模块和网络接口配置、设备链路的使用、设备上运行的网络协议和网络管理工作站等做出规定。

进行交换机参数配置有两种途径：通过与交换机控制台端口连接的计算机作为本地控制台进行配置和通过网络登录作为远程控制台进行配置。

4. 实施注意事项

在网络实施任务中的注意事项如下：

- 选择资质合格的施工单位。
- 加强工程协调。
- 照顾后续施工步骤。
- 把好产品关。
- 把好工程质量关。
- 特别关注光纤布线。
- 注意布线系统的防火。
- 重视屏蔽布线系统的接地问题。

在布线实施过程中，施工部门必须对所安装的线缆系统进行相关标准的测试以保证质量的可靠性。

3.1.1.2 测试

测试工作伴随着整个网络工程的全过程，无论是布线安装还是系统调试，都需要进行反复的测试和确定。

1. 测试计划

测试计划应包括下列 5 个方面的内容：

(1) 简要说明

简要说明包括工程的概况和需要达到的主要指标。

(2) 测试内容

逐项列出测试的步骤、名称、内容和预期达到的目标。

(3) 测试清单

对每项测试内容列出测试的部位和参与测试的单位，包括进度的安排、测试工具和相应的条件(设备和软件等)。

(4) 测试设计说明

测试设计说明是对每项测试内容的测试设计考虑，应包括测试的控制方式、输入条件和预期的输出结果。

(5) 评价准则

说明测试所能检查的范围及其局限性，以及用来判断测试工作是否通过的评价尺度，包括合理的输出结果、测试输出结果与预期输出结果之间容许出现的偏差范围。

测试工作完成后，应提交一份《测试分析报告》。测试分析报告主要包括下列内容：概要说明、测试结果、结论、原因分析、建议和评价。

2. 网络测试

网络测试是对网络设备、网络系统以及网络对应用的支持进行检测，以展示和证明网络系统能否满足用户在性能、安全性、易用性、可管理性等方面需求的测试。网络测试的实施一般包括以下环节：

- 根据测试目的，确定测试目标。
- 在对相关网络技术和实现细节透彻掌握的基础上，设计测试方案。
- 建立网络负载模型。
- 配置测试环境，包括测试工具的选择及必要的测试工具的研发。
- 采集和整理数据。
- 分析和解释数据。
- 准确、直观、形象地表示测试结果。

网络测试包括网络设备测试、网络系统测试和网络应用测试 3 个层次。

(1) 网络设备测试

网络设备测试主要包括以下几个方面：功能测试、可靠性和稳定性测试、一致性测试、互操作性测试和性能测试等。

① 功能测试验证产品是否具有设计的每一项功能。

② 可靠性和稳定性测试往往通过加重负载的办法来分析和评估系统的可靠性和稳定性。

③　一致性测试验证产品的各项功能是否符合标准。

④　互操作性测试考察一个网络产品是否能在一个不同厂家的多种网络产品互联的网络环境中很好地工作。网络产品不同于其他产品的最大特点是必须符合标准，不同的网络产品之间要能互操作。

⑤　性能测试的主要目标是分析产品在各种不同的配置和负载条件下的容量和对负载的处理能力，如交换机的吞吐量、转发延迟等。

典型的网络设备性能测试方法有两种：第一种方法是将设备放在一个仿真的网络环境中进行测试；第二种方法是使用专用的网络测试设备对产品进行测试。

(2)　网络系统和应用测试

网络系统测试除了普通意义上的物理连通性、基本功能和一致性的测试以外，主要包括网络系统的规划验证测试、网络系统的性能测试、网络系统的可靠性与可用性的测试与评估、网络流量的测量和模型化等。

①　网络系统的规划验证测试主要采用的两个基本手段是模拟和仿真。

- 模拟是通过软件的办法，建立网络系统的模型，模拟实际网络的运行。通过设定各种配置和参数模拟系统的行为，对系统的容量、性能以及对应用的支撑程度给出定量的评价。这对于大型网络的规划设计是不可缺少的环节。
- 仿真是指通过建立典型的试验环境，仿真实际的网络系统。规划验证测试的目的在于分析所采用网络技术的可行性和合理性，网络设计方案的合理性，所选网络设备的功能、性能等是否能够合理地有效地支持网络系统的设计目标。

②　网络系统的性能测试是指通过对网络系统的被动监测和主动测量确定系统中站点的可达性、网络系统的吞吐量、传输速率、带宽利用率、丢包率、服务器和网络设备的响应时间、哪些应用和用户产生最大的网络流量，以及服务质量等。此项工作同时可以发现系统的物理连接和系统配置中的问题，确定网络瓶颈，发现网络问题。测试设备记录一段时间内的网络流量，实时和非实时地分析数据。被动测量不干涉网络的正常工作，不影响网络的性能。主动测量向网上发送特定类型的数据包或网络应用，以分析系统的行为。

③　网络应用层次上的测试则主要体现在测试网络对应用的支持水平，如网络应用的性能和服务质量的测试等。例如部署基于 IP 的语音传输 VoIP 时，最直接的问题是网络中的交换机和路由器设备能否有效地支持语音传输、网络能支持多大的语音流量、多少个语音通道；如果网络支持 VoIP，对网络的其他业务特别是关键业务，会产生什么样的影响；网络是否支持服务质量 QoS。这些问题都需要通过网络测试来回答。

④　网络系统测试的核心工具是协议分析仪。这是一种专用的网络测试设备，它能够连接到网络上，产生并向网上发送数据、捕捉网上数据、分析数据。协议分析仪一般具有网络监测、故障查找、协议解码和流量产生等功能。

⑤　网络流量的测量和模型化。网络流量的测量和模型化对于分析网络性能和带宽的利用率，指导网络流量管理，开发高效的网络应用十分重要。这方面的工作主要有：

- 产生已知特征的流量，使该流量沿网络传播，最后回到测试仪。记录和分析流量特性的任何改变(如延迟漂移)。
- 对链路总体流量的测量和传输时间、吞吐量、带宽利用率等的分析。
- 分析特定流量的特征和提供的 QoS；收集一个时间段的测量数据进行分析，分析

流量沿网络传播过程中流量特征的变化和网络流量的统计行为，建立流量模型。

3. 网络安全性测试

现在有很多新型网络设备尤其是网络边缘路由器增加了防护功能，阻止了人为、故意的网络攻击。然而提供的防护会不会对正常数据转发造成影响？有什么样的影响？这些很难从理论上估计，需要进行必要网络设备安全性测试。

本节提到的测试项验证网络设备提供的基本安全功能，并检测这些安全功能项对网络设备运行造成的影响，这些测试项分为访问列表测试和 DOS 攻击测试两大类：

(1) 访问列表测试

访问列表测试是检测边缘路由器的访问列表能否起到防火墙的作用，控制网络传输过滤数据报文，阻止或允许数据报文通过网络接口。过滤依据可以是源地址、目的地址、上层协议号。边缘路由器通过将进入或离开的数据报文与访问列表中过滤项比较，决定允许或阻止数据报文通过。边缘路由器能提供的访问列表容量，以及不断变化的访问列表对数据转发的影响都要进行测试。

(2) DOS 攻击测试

DOS 攻击测试是检测边缘路由设备抵抗“拒绝服务(DOS)攻击”的能力。当设备由于伪造的服务请求和虚假的传输而变得非常繁忙时，就无法响应正常的服务请求，从而造成损失。DOS 攻击测试考验网络设备检测并阻止某种特定攻击的能力，并检测受到某种攻击设备超负荷运行情况下，正常传输转发性能受到的影响。

具体的安全性测试项目如下：

- 访问列表性能测试
- 虚假源地址攻击测试
- LAND 攻击检查
- SYN 风暴检查
- Smurf 攻击检查
- Ping 风暴检查
- Teardrop 攻击检查
- Ping to Death 检查

4. 性能测试

性能测试包括可靠性测试、功能/特性测试、吞吐量测试、衰减测试、容量规划测试、响应时间测试、可接受性测试和网络瓶颈测试等。

(1) 可靠性测试

可靠性测试是使被测网络在较长时间内(通常是 24~72 小时)经受较大负载，通过监视网络中发生的错误和出现的故障，验证在高强度环境中网络系统的存活能力，也就是它的可靠性。可靠性测试可作为接受性测试的一部分，在产品评估测试中可作为比较测试或作为产品升级进行的衰减测试的一部分。采用的负载模式很重要，越贴近真实负载模式越好，可靠性测试中使用网络分析仪监控网络运行、捕获网络错误。

通常在较长时间段内和持续负载下，不同网络具有不同级别的存活度。如果测试时间足够长、负载足够大，所有可靠性测试最终都会失败。

可靠性测试用于网络生命周期中的以下 3 个阶段：

- 计划　作为产品评估测试的一部分，比较不同产品或建立要求规范。
- 开发　验证计划中的要求是否在系统中完全实现。
- 组建　该测试作为可接受性测试的一部分，在网络运行前进行，核实系统是否达到要求。

(2) 功能/特性测试

特性测试核实的是单个命令和应用程序功能，通常用较小的负载完成，关注的是用户界面、应用程序的操作以及用户与计算机之间的互操作。特性测试通常由开发人员在他们的工作台上完成，或是在一个小型网络环境下由测试人员完成。

功能测试是面向网络的，核实的是应用程序的多用户特征和在重负载下后台功能能否正确地执行，关注的是当多个用户正在运行应用程序时，网络和文件系统或数据库服务器之间的交互。功能测试要求网络的配置和负载非常接近于运行环境下的模式。该测试可以在运行网络或独立网络实验室里完成。它只应用于网络生命周期中的以下 3 个阶段：

- 开发　核实在期望的运行模式下，在多用户环境里，应用程序的运行性能是否达到要求。
- 组建　在应用程序安装前完成，可独立进行也可作为接受性测试的一部分，用于核实在期望的运行模式下，应用程序的运行性能是否达到要求。
- 运行　该阶段测试是在应用程序运行后进行的，如果在运行系统中遇到了问题，该阶段测试用于核实应用程序是否如最初应用时那样工作。

(3) 吞吐量测试

吞吐量测试和应用程序的响应时间测试相似，但检测的是每秒钟传输数据的字节数和数据报文数，而不是响应时间。用于检测服务器、磁盘子系统、适配卡/驱动连接、网桥、路由器、集线器、交换器和通信连接。吞吐量的测试用于测量网络的性能，找到网络瓶颈以及比较不同产品的性能。

吞吐量测试不使用程序脚本，它借助某些软件对网络服务器执行文件输入/输出操作来产生流量，或通过某些软件在网上发送专门的数据报文或帧。该测试被用于网络生命周期的以下几个阶段：

- 计划　用于比较网络产品，为模拟网络节点提供运行特征和要求规范。
- 开发　用于核实网络组件以及整个网络是否达到规范的要求水平。
- 组建　可独立进行的或作为可接受性测试的一部分，在网络组件或整个网络正式运行之前核实它们是否满足规范的要求。

(4) 衰减测试

衰减测试是将硬件或软件的新版本与当前版本在性能、可靠性和功能等方面进行比较，同时验证产品升级对网络的性能不会有不良影响。衰减测试混杂了很多为完成其他测试任务要进行的测试。衰减测试的关键是要保证被测组件应是运行网络中最关键或最脆弱的组件。

该测试不强调升级版的新特性。新特性测试在衰减测试之前作为功能/特征的一部分就已完成。尽管新产品应该解决了当前版本中的错误，但它们也经常存在一些以前没有出现过的错误，如果这些错误发生在产品的关键部分，将会引起严重问题。衰减测试不需要测

试产品的所有特性，但网络用户正常运行所依靠的关键功能必须在测试之列。

衰减测试应用于网络生命周期的以下两个阶段：

- 开发　测试核实产品升级版是否能满足性能、互操作性和可靠性的要求。
- 升级　在采用升级版本之前用该项测试来比较升级版和当前版，看升级版是否和当前版本一样满足性能、互操作性和可靠性的要求。

(5) 容量规划测试

容量规划测试可检测当前网络中是否存在多余的容量空间，当网络承受的总负载超过网络总容量时，网络的性能或吞吐量就有可能下降，所以在网络负载接近这一临界点(网络的最大容量)前，就要根据负载增长的幅度扩充网络资源。

进行该项测试要逐渐增加网络负载，直到网络的运行性能、可接受的水平或吞吐量不断下降，达不到设计所要求水平为止。网络运行负载和网络最大吞吐量之间差额就是现有系统的冗余量。

容量规划测试被用于网络生命周期的以下 3 个阶段：

- 计划　用于估计实施该系统所需要的资源，也可用于成本分析和制定预算。
- 开发　检测系统要求的资源是否满足特定的响应时间和吞吐量的要求。
- 升级　当系统响应时间或吞吐量下降时，重新选取网络组件。

(6) 响应时间测试

响应时间测试是检测系统完成一系列任务所需的时间，本项测试是用户最关心的，对于表示层，如微软的 Windows，该测试是指在不同桌面之间切换或装载新负载所需的时间。在不同负载即不同实际或模拟用户的数目下运行这一实验，对每个被测试应用程序生成一个负载-响应时间曲线。

在应用程序测试中，执行一系列典型网络动作的命令，如打开、读、写、查找和关闭文件，这些命令提供了最好的负载模拟。例如，对每个进行测试的工作站，检测它在几秒内能完成这些命令。

响应时间测试应用于网络生命周期的以下几个阶段：

- 计划　使用模拟应用程序进行，检测规范要求的各项网络服务。
- 开发　检验规范要求的网络服务是否正在被实现。
- 组建　接受和组建之前，核实规范要求下的网络服务是否已经被实现。
- 运行　检测网络服务的基准和变化，这可能是针对系统质量的最好测试。

响应时间测试应该包括对系统可靠性的检测。常见的可靠性问题例如，在路由器或服务器中大量丢失数据报文或由于网络组件故障引发的大量坏数据报文，这一切都将严重影响网络的响应时间，因此在整个测试期间都应用网络分析仪监视系统错误。

(7) 可接受性测试

可接受性测试是在系统正式实施前的“试运行”。它是一个非常有效的方法，确保新系统能提供良好而稳定的性能。和衰减测试一样，可接受性测试中也包含多项测试，例如：响应时间、稳定性和功能/特性测试。

可接受性测试在许多领域都有使用，而在安装或升级网络前应进行的网络可接受性测试则经常被忽略，而事实上可接受性测试能为网络购买者在经济上和技术上提供有力保证和参考。

可接受性测试可以仅在新增加的部件上完成，将已存在的负载加上新增程序或新增组件可能产生的负载作为测试使用的负载。可接受性测试应用于网络生命周期的以下两个阶段：

- 开发　该测试在开发阶段前定期执行，用来核实要求的标准是否可行。
- 组建　该测试用于在网络投入运行之前，核实系统是否满足所有要求。

(8) 网络瓶颈测试

网络瓶颈测试可以找到导致系统性能下降的瓶颈。测试中需要测试和计算系统的最大吞吐量，然后再在单个网络组件上进行该项测试明确各自的最大吞吐量。通过计算单个组件的最大吞吐量和系统最大吞吐量之间的差额，就能发现系统瓶颈的位置以及哪些组件有多余容量。

系统瓶颈在不同的测试案例中，出现的位置可能有所变化。例如，一个客户业务应用程序测试可能表明服务器是系统的瓶颈，而对一个电子邮件系统的测试可能表明广域网连接才是网络的限制因素。如果可以在测试的环境中重现引起问题的负载，那么这样的测试结果对解决问题将有巨大帮助。瓶颈测试用于网络生命周期的以下两个阶段：

- 组建　可以作为容量计划的一部分，用于帮助相关人员明确影响网络性能和响应时间的瓶颈位置。
- 运行　作为故障检测的一部分帮助找出影响网络性能或引起系统问题的网络瓶颈。

5. 测试报告

测试报告是整个项目的第一份供大家交流和领导查阅的报告，人们对工程满意程度和对工程质量的认可很大程度上来源于这份报告。通常在独立网络测试实验测试后，要总结测试数据，并基于此对测试过的同类产品进行排序；而系统内部的测试仅是得出一个简单的结论。

测试报告呈现的内容和采取的表现形式非常重要，通常测试报告包含以下信息：

- 测试目的　用一句或两句话解释本次测试的目的。
- 结论　从测试中得到的信息和推荐下步的行动。
- 测试结果总结　对测试进行总结并由此得出结论。
- 测试内容和方法　简单地描述测试是怎样进行的，应该包括负载模式、测试脚本和数据收集方法，并且要解释采取的测试方法怎样保证，测试结果和测试目的相关，以及测试结果是否可重现。
- 测试配置　网络测试配置用图形表示出来。

测试报告的形式可以是一个简短的总结(2~4 页)也可以是很长的书面文档(5~20 页)。测试总结可以使用图形表示测试结果，例如应用程序的响应时间、吞吐量和产品评估。而系统衰减性测试、配置规模和应用程序的功能/特性测试的测试报告还要包括更多的信息。

在非常特殊的情况下，测试报告需要长达 50 页的测试报告。它通常包括从项目开始到结束按时间编排的所有活动，以及非常详细的问题信息和解决问题的信息。

6. 网络测试工具

一般网络的测试工具包括：

- 网络管理和监控工具
- 建模和仿真工具
- 服务质量和服务级别管理工具

网络管理和监控工具如 HP 公司的 Open View，能够在网络测试运行过程中提示某些问题的网络事件的出现。这些工具可以是驻留在网络设备中的应用软件。例如，Windows 2000 网络操作系统中包含了监测服务器的 CPU 利用率，发送接收分组的速率和内存使用情况的功能等，这些功能能够帮助发现和识别网络设计中的性能问题。

协议分析仪也能被用于监测新设计的网络，帮助分析通信的行为、差错、利用率、效率以及广播和多播分组。

建模工具和仿真工具是更为先进的用来测试验证网络设计的工具。仿真就是在不建立实际网络的情况下，使用软件和数学模型来分析网络行为的过程。利用仿真工具，可以根据所需要测试的目标开发一个网络模型，从而估计网络性能并对各种网络实现的方法之间的差异进行比较。仿真工具使得选择比较的空间变得更大，特别适合于实现和检查一个扩展的原型系统。一个好的仿真工具往往非常昂贵，实现的技术也比较复杂，它要求开发人员不但要精通统计分析和建模技术，而且还要对计算机网络有所了解。

服务级别管理工具是一种比较新型的工具，主要用来分析网络应用的端到端性能。有些工具能够管理服务质量和服务级别，有些工具能够监控实时应用的性能，有些工具能够预测新的应用性能，有些工具可以将上述功能结合起来实现更强大的功能。

3.1.1.3 评估

评估测试不只针对物理设备，更重要的是要评估、比较各种网络技术。通常使用模拟测试配置和模拟负载进行子系统(如路由器)和网络技术(如 ATM 或 FDDI 等)的评估。评估测试不适用于全局网络，因为全局网络拓扑负载、网络设备太多，不好准确定位引起问题的原因和位置，不能进行有效的比较，多数评估测试在专用的子网测试环境中进行。

很多公司都有其固定合作的网络设备供应商，如路由器、集线器或交换机的供应商。通常很少再做设备比较测试，但网络技术的比较测试需要经常进行。企业经常面对选择哪种技术以及怎样比较不同技术的问题，所以技术评估是评估测试中很重要的一项。

在比较设备与技术时，除了使用专用于待测设备或技术的工程负载外，有经验的程序员也使用真实负载，使用真实负载可以了解待测设备或技术在特定环境下的运行性能。通过两种负载模式检测结果的比较，可以获知待测设备还有多少多余容量。

评估测试与设备或技术的特性、功能测试一样，比较待测设备或技术的性能、稳定性、特性、易用性配置和管理等方面的功能。

评估测试实质是衰减测试的基础，评估测试中对几种设备或技术进行比较；衰减测试中对同一设备的不同版本进行比较。测试中选择设备的标准也完全可作为验证升级版本工作正常与否的标准。尽可能多地集成在计划/设计阶段进行测试是非常好的方法，最初的产品评估测试可以被开发阶段的可接受性测试和升级阶段的衰减性测试所借鉴。

评估测试是最常进行的测试，在设备选型、技术选型，以及网络系统升级过程中都要进行或多或少的评估测试。

用于评估测试的负载模式和测试脚本要能有效覆盖被检测设备和技术。常使用最好情

形(工程负载)和真实负载模式进行测试，两种方式都提供了惟一的、重要的检测结果，测试人员要能够理解、解释它们测试结果间的不同。

工程检测结果是被测设备和技术在最理想的情形下测试得到的结果，因此不能在真实运行环境里显示它们的运行性能；真实检测结果能很好地显示待测设备或技术在运行网络环境中的性能，但无法预测设备的总容量。如果时间允许，两种测试都要做。通常测试人员只有时间进行一种测试，一般进行最好情形的测试。许多公开发行的测试报告都是基于最好情形(工程负载)下的测试结果。

所有的测试配置都是模拟的。用于设备比较的测试配置不一定要代表运行网络的典型配置，任何有效、公正的测试配置都能对被测产品进行很好的比较。然而测试配置和负载越接近运行网络的配置和负载，测试的结果越能反映被测设备在运行网络中的运行情况。

在安装和配置测试网络时必须注意：确保配置中所有测试组件都是最新版本的；使测试尽可能的公正和统一，以取得最好的测试结果。在测试非正式版时一定要小心，因为发布日期经常有错误，测试配置中安装了非正式版后，它还可能会变，所以非正式版的测试结果和正式版的测试结果经常不一致，分析非正式版的设备经常会延误项目的进行。

进行评估测试时，除了被测设备，测试配置中的所有网络组件要保持不变。这一点非常重要，只有这样才可以保证被测设备可以进行公平比较。对于子网，这一点很容易做到(一个网络设备很容易被另一个设备替代)。

网络技术评估要比较各种网络技术，因而测试配置中的几个网络组件都需要更换。重要的是不要改变源或目标配置。在配置中不仅通信线路需要更换，路由器也需要更换。传输负载和端点的配置要保持不变。

评估测试计划中的各个测试任务，逐步完成进行测试、数据收集和数据解释。在评估测试中各测试进行的先后次序没有关系，因为它们不是线性关系，而是多次重复进行的。当在测试中发现了新的信息，以前做的测试可能要重新进行，确定它的测试结果或对以前的测试稍做改变以检验网络运行的其他方面。此外在评估期间设备提供商经常发布新的版本或非正式的版本，所以各种基于这种设备的测试要重新进行。

制定网络设备、技术比较或取舍标准时，不仅要参考评估测试所得测试结果数据，还要综合考虑其他一些信息，如各设备的性能价格比，但没有运行网络的持续和峰值负载要求，所以缺少比较基准，往往将产品评估测试引入歧途。

最终根据评估测试所得的数据和图表对网络系统做出总结性评估，并撰写网络系统评估报告。

3.1.1.4 转换到新网络的工作计划

转换到新网络是一件复杂的过程，需要仔细筹划，推荐按以下步骤进行：

1. 评估

在转移到系统以前，首先对系统进行测试，即将本单位的主要软件迁移至新网络上进行运行测试，查看测试结果并记录下系统是否符合建议书中的要求。要特别注意新用户的登录界面、重要应用软件的运行方式、系统的响应时间、升级带来的新特征。这种方案确保测试是对软件的全面测试。

2. 训练

如果由上一阶段的结果确定新网络是可行的，那么可以全面投入使用。接下来就是制定培训计划，培训在新网络环境中的用户和管理员。

3. 预实施

预实施作为实施迁移的第一步，应该细化迁移计划书中的时间表和计划表，使它成为实施迁移的详细的工程计划。在计划书中，确定需要迁移的用户标识名。查看已存在的服务器，决定哪个设备、文件、目录应该被移植，哪些应被压缩。在迁移到新网络之前，需要提前通知所有用户做好准备。

4. 迁移

选择一个适当的迁移时间，最好定在单位事务不繁忙的时候(如周末)，事先做好系统软件和数据的备份，然后逐步将原有系统安装部署到新网络中，并作好相关设备的配置。要一边安装一边测试，注意不但要用管理员身份测试，还要使用普通用户身份测试，确保迁移后的系统与原有系统一致。

5. 迁移之后

当网络迁移工作完成之后，要开放网络的登录，通知用户新网络开通。要仔细回顾升级过程，以便总结教训能更有效地升级其他服务器，减少遇到的麻烦。努力理解由升级产生的各种支持要求。继续测试新的系统，在必要的时候优化系统，争取在对用户造成问题之前，就排除它们。

当发现某部分迁移后影响了原有功能，在无法迅速解决问题之前，可以暂时撤消迁移而继续采用原有系统。

3.1.2 典型例题分析

例 1 什么是系统集成？它有哪些具体任务？有何优点？

分析：系统集成是在一定的系统功能目标的要求下，把建立系统所需的管理人员和技术人员、软硬设备和工具，以及成熟可靠的技术，按低耗、高效、高可靠性的系统组织原则加以结合，使它们构成解决实际问题的完整方法和步骤。

系统集成实施的具体任务随每个项目的不同而变化。一般来说，可将其具体工作细分如下：系统逻辑结构图的设计、项目及分包商的管理、硬件和软件产品的采购、开发环境的建立、应用软件的开发、应用系统的安装、测试、实施和培训。

系统集成的优点包括：责任的单一性(最终客户面对的仅仅是一个系统集成商)、客户需求得到最大限度的满足、系统内部的一致性得到最大限度的满足、系统集成商保证客户得到最好的解决方案(避免独立的厂商为自身利益而将其产品过多地挤进系统)。

答案：略。

例 2 下面哪一种办法可以消除以太网阻塞？

(1) 启用全双工以太网。

(2) 在以太网络中冲突难以彻底避免。

(3) 启用半双工以太网。

(4) 将共享 Hub 全部替换成以太网交换机。

(5) 创建 VLAN。

分析：消除阻塞的惟一办法是使用全双工以太网。全双工的以太网允许一个工作站同时发送和接收数据。以太网的交换机减少了阻塞的可能性，但是，如果一个设备处于半双工状态，它就有可能存在同时接收和发送的情况，这就可能造成阻塞。

答案：启用全双工以太网。

例3 各种测试任务在网络的整个生命周期中是如何分配的？

分析：测试工作应当贯穿于网络的整个生命周期中，只有经常测试才能保证对网络运行现状有一个准确的了解，才能更好地维护网络的稳定性。在网络生命周期中，不同的阶段应当实施不同的测试任务，具体如表 3.1 所示。

答案：网络生命期各阶段的测试任务如表 3.1 所示。

表 3.1 测试任务表

层 次	测试任务	规划设计	开 发	实 施	运 行	升 级
网络应用/表示层	应用程序响应时间	√	√	√	√	
	应用程序功能/特性		√	√	√	
	衰减		√			√
	吞吐量	√	√	√		
	可接受性		√	√		
	配置规划		√			√
	稳定性	√	√			
	产品评估	√				
	容量规划			√		√
	瓶颈识别				√	
网络系统层	应用程序响应时间					
	应用程序功能特性					
	衰减		√			√
	吞吐量	√	√	√		
	可接受性		√	√		
	配置规划	√	√			√
	稳定性	√	√			
	产品评估	√				
	容量规划			√		√
	瓶颈识别				√	

例4 如何进行交换机的参数配置？

分析：进行交换机参数配置有两种途径：通过与交换机控制台端口连接的计算机作为本地控制台进行配置，通过网络登录作为远程控制台进行配置。在第一次对交换机进行配置时，由于交换机的网络登录功能还没有打开，因此只能够通过本地控制台进行配置。交

换机的一般配置过程如下:

(1) 打开本地控制台。

(2) 登录到交换机。

(3) 进入配置工作模式(有命令模式和向导模式两种方法)。

(4) 为交换机命名。

(5) 口令设置。

(6) 进行交换机功能配置。

下面以 Windows 系统平台为例,说明将个人计算机连接到交换机的操作方法。

(1) 首先使用串行线缆或专用转换线缆,将计算机的串行端口 COM1 或 COM2 与交换机的控制台(Console)端口连接。

(2) 交换机加电启动。

(3) 在 Windows 系统中单击【开始】|【程序】|【附件】|【通信】|【超级终端】命令,运行 Hypertrm.exe。

(4) 为新建立的终端连接命名,然后单击【确定】。

(5) 根据使用的串行接口,为终端选择连接方式。

(6) 配置通信参数为 9600 波特率、8 个数据位、1 个停止位和没有奇偶校验,单击【确定】后若连接正常,会出现超级终端运行窗口,按 Enter 键就会出现交换机的操作提示符。

在局域网中常见的配置内容如下:

- 设备 IP 地址配置
- 端口配置
- VLAN 配置
- 生成树协议配置
- 链路聚合配置
- 路由协议配置
- 静态路由配置
- 网络管理配置

交换机安装配置完毕以后,就可以加电调试了,根据调试结果可以调整配置,以满足用户需要。

答案:略。

3.1.3 同步练习

1. 第 3 层交换机哪些功能可用在接入层?

2. 指出哪些设备出现在各模块中(注意一些设备可能出现在多个模块中):

模块:

电子商务模块 因特网连接模块 远程接入与 VPN 模块

设备:

Web 服务器 SMTP 邮件服务器 防火墙 网络入侵检测系统(NIDS)工具

DNS 服务器　VPN 集中器　公共 FTP 服务器

3. 综合布线时经常出现的故障有哪些?

4. 配置输入 Cisco 2509 的 IOS 配置命令。进入虚拟操作平台后，在 IOS 环境下输入了如下的配置，请解释(1)~(4)处的标有下划线部分配置命令的含义(“◇”后为配置内容，“★”和“//”后为注释内容)。

```
★ 配置服务器信息
◇ hostname Cisco 2509          //服务器名称
◇ enable secret******          //特权口令
◇ ip domain-manl wxx.edu.cn    //设置拨号服务器所属域名
◇ ip-name-server 202.112.77.2 //设置拨号服务器 DNS
(1) (此处有 3 条下划线)
◇ async-bootp subnet-mask 255.255.255.0
◇ async-bootp gateway 202.112.77.254
◇ async-bootp dns-server 202.112.77.2
★ 配置 Ethernet Port (略)
......
★ 配置动态分配的地址池
◇ ip local pool pool2509 202.112.79.1 202.112.79.8  //定义 IP 地址池
★ 配置 Asynchronous Interface
                                //异步口是 RAS 服务器上连接 Modem，用于用户拨号的端口
◇ interface Group-Async 1 //对第一组异步接口进行配置，对异步口的配置可以按组，也
                            可以按单个口
group-range 1 8                 //划定 1 到 8 号异步口属于第一组
encapsulation pap               //加载点到点协议
(2) (此处有 2 条下划线)
ansync dynamic address
ansync default address pool pool2509 //pool2509 的定义见“配置动态分配的地
                                      址池”部分
ppp authentication pap  //设置 PPP 的验证方式为用户口令方式
★ 配置 router 信息
(3) (此处有 3 条下划线)
◇ router rip
network 202.112.77.0
network 202.112.79.0
★ 配置拨号服务器的默认路由(略)
......
★ 配置存取用户组
◇ access-list 1 pormit 202.112.77.0.0.0.255  //定义用户组的范围
★ 配置 Asynchronous PORT (略)
★ 配置 vty
◇ line vty 0 4  //配置虚拟终端
(4) (此处有 3 条下划线)
access-class 1 in  //access-class 的定义见“配置存取用户组”
password ******
login
```

3.1.4 同步练习参考答案

1. 可用在接入层的一些第 3 层交换机功能为：

- 广播域(包括 VLAN)之间的路由选择
- 使用不同的广域网技术访问远程办公室
- 路由传播
- 分组过滤
- 验证与安全性
- 服务质量(QoS)
- 按需路由选择(DDK)和静态路由选择

2. 电子商务模块：Web 服务器、防火墙、网络入侵检测系统工具。

因特网连接模块：SMTP 邮件服务器、防火墙、公共 FTP 服务器、DNS 服务器。

远程接入与 VPN 模块：VPN 集中器、网络入侵检测系统工具、防火墙。

3. 对于光纤媒体而言，最常见的故障是因光纤断裂、破损或老化而引起的，造成这些故障的原因主要有：

- 光缆保护套磨损导致光纤因挤压而断裂。
- 光缆过分弯曲(超过所允许的弯曲半径)致使光纤断裂。
- 光纤长期暴露在 α 或 γ 射线下。

光纤连接器也是经常产生故障的地方，这主要是由于安装质量太差或者使用维护不当所致。引起光纤连接器故障的因素包括：

- 连接器的连接不紧密。
- 连接器中的纤芯断裂。
- 光纤接口不吻合。
- 光纤接口磨光不精确。
- 连接器保险装置故障。

对于双绞线媒体来说，安装不当造成的危害可能会更大，甚至还会出现某些隐性错误。如双绞线电缆的磨损可能并没有直接断开，而是阻抗增大，到一定程度才会危及系统工作。双绞线连接器的安装是最容易引发故障的地方，由于双绞线的对数较多，错误的安装也就经常会发生。引起双绞线安装故障的原因主要包括：

- 电缆的磨损造成双绞线断路或阻抗加大。
- 连接器型号使用不当(如用 RJ-11 代替 RJ-45)。
- 双绞线的极性不正确(参见第 6 章的描述)。
- 线路缠绕产生近端串扰。
- 配线总长度超过了规定范围。

需要特别提醒注意的是，在结构化布线时，由于线路沿墙壁绕行，线路拐弯抹角将增加很大的开销，总长度的计算必须精确。

4. 配置命令的含义如下：

(1) 配置 RAS(Remote Access Server)的拨号用户网络配置信息。包括用户默认子网掩码、默认网关、默认 DNS。当用户拨入时，服务器自动将配置信息传递给用户。

(2) 设定第一组异步口的用户 IP 地址自动分配。设置自动分配的 IP 地址来自于 IP 地址池 pool2509。

(3) 配置路由协议 RIP。指定设备直接连接到网络 202.112.77.0 与 202.112.79.0。

(4) 设置来自 202.112.77.0 网段的用户可以访问拨号服务器，配置用户登录口令。

3.2 本 章 小 结

网络系统的具体实施阶段的主要工作是构建网络和测试网络。如何按照网络系统的设计方案进行实施，保证网络建成后能够符合设计目标，是网络建设中较为关键的内容。因此需要在网络实施过程中，加强过程的监控，按照施工规范进行线路的铺设和设备的安装调试，在网络建成后还需要制定详细的测试计划，进行性能、可靠性和安全等多方面的测试工作，对网络系统的可用性进行评估，判断它是否达到预期目标。网络建成后，需要制定周密的工作计划，做好将企业应用从旧的网络系统向新系统迁移的工作。

本章重点是对网络系统进行测试，包括连接测试、安全性测试、性能测试。

第 4 章　网络系统的运行和维护

大纲要求：

- 用户措施　用户管理、用户培训、用户协商。
- 制定维护和升级的策略和计划　确定策略、设备的编址、审查的时间、升级的时间。
- 系统维护的高可靠性技术。
- 维护和升级的实施　外部合同要点、内部执行要点。
- 系统容错技术。
- 存储、备份与数据恢复　数据的存储、备份、数据恢复。
- 网络系统的配置管理　设备管理、软件管理、网络配置图。

4.1　网络系统的运行和维护

4.1.1　考点辅导

4.1.1.1　用户措施

1. 用户管理

用户(user)是网络系统的主要使用者，使用网络的单位和个人都属于用户范畴。用户的身份决定其在网络系统中的权限，因而在网络系统中担任不同的角色(role)。

在网络中必须有严格的用户管理措施，才能保证网络的正常使用和运转。系统管理员是网络系统的维护人员，他的重要任务之一就是管理用户，他本人也是用户，但拥有比其他用户更高的权限。

用户在使用网络系统之前需要注册，即将用户信息提交给网络管理员审阅，通过后即可开通服务。用户使用网络资源的过程中必须接受管理员的管理和网络管理程序的控制，用户的行为必须遵守既定网络管理规则。

网络用户管理包括以下内容：

(1) 局域网用户管理　局域网用户的创建、注销和访问权限管理，主域用户资料数据库的维护和管理。

(2) 电子邮件用户管理　电子邮件用户开户审核，用户创建、注销和权限管理，电子邮件用户数据库的维护。

(3) 用户入网设备 IP 地址管理　局域网用户的 IP 网络地址分配和技术支持，用户 IP 地址分配数据库的维护。

(4) 用户 Internet 访问管理　Internet 访问权限管理、传输内容监控和费用分配控制管理，用户流量数据库管理和维护。

在局域网环境中存在多种网络应用和管理系统，每个系统都含有一套独立的用户身份认证管理系统。为了有效地管理用户信息并利用这些信息提高网络管理效率，需要建立统一身份认证系统，目前用户信息管理系统大都建立在轻量目录访问协议(Lightweight Directory Access Protocol，LDAP)基础之上。

2. 用户培训

用户培训是保证系统正常运行的重要因素，需要针对不同层次的用户进行不同内容的培训。用户培训需要经过以下几个过程：

(1) 培训需求　调查哪些用户需要培训。

(2) 需求分析　进一步分析用户的培训需要，总体设计培训流程。

(3) 课程定制　针对不同的用户制定不同的课程计划和授课内容、预期目标等。

(4) 确定师资　选择有经验的教师教授课程，教师必须熟悉课程及相关内容。

(5) 培训实施　确定培训时间段和授课计划。

(6) 信息反馈　及时对培训效果进行调查，以便调整后期培训方案。

用户培训是一个不断完善的过程，每一期的培训经验都应带入到下一次培训作为参考。随着网络系统的升级和大量网络新技术的使用，用户培训需要经常开展，以便用户能够更好地了解和使用网络服务，最大限度地发挥网络效益。

3. 用户协商

用户的要求永远都是网络存在的依据，所以网络系统提供的服务必须随时能够满足用户的需要，用户对于网络系统的服务质量的意见，都应该认真听取并尽量改进。应该定期征求用户的意见和要求，可以通过问卷或召开会议的方式，征求他们对于系统运行状况及可能的发展方向的意见，作为以后维护和升级的参考依据。

4.1.1.2　制定维护和升级的策略和计划

网络维护是保障网络正常运行的重要方面，主要包括设备保养与维护、故障检测与排除、网络日常检查、网络性能监控及网络升级等。此处只介绍网络升级知识，其他部分将在第 5 章中详细介绍。

1. 确定策略

当网络出现性能下降、技术老化、用户业务规模扩展时，就意味着原有网络不再满足用户需要，此时网络必须进行升级。升级前需要确定升级的策略。

升级的步骤包括：

(1) 评估并确定需求　了解网络环境的运行现状，分析升级的原因。

(2) 制定目标　确定升级要实现的目标。

(3) 制定预算　根据升级的目标确定升级需要更换的部件，根据市场价格制定预算。

(4) 制定规划　详细描述升级计划并形成文档。

(5) 测试规划　对升级计划的可行性进行测试，在必要时调整升级计划。

(6) 用户培训　对升级涉及的用户进行培训，让他们熟悉新系统。

(7) 备份与恢复　在升级前对系统文件和数据进行备份，升级失败时恢复系统。

(8) 实施升级 按照升级计划的内容严格执行升级。

(9) 检查实施情况 评估升级是否达到既定目标。

2. 设备的编址

在升级的过程中需要对使用的设备(如服务器、工作站、路由器等)进行编址，即给每个设备分配一个 IP 地址，并详细记录每个 IP 所对应的部门、位置、机器编号和 MAC 地址等，存入 IP 地址管理数据库，并规定用户不得任意更改以避免 IP 地址冲突。设备的编址也应遵循一定规则，比如可以按照部门、位置或机器的型号等进行编址，具体应由网络管理员根据实际情况确定。另外，每个部门 IP 地址应留有一定的空余，以备今后添加设备之用。

3. 审查的时间

升级规划的审查时间应在升级实施之前，审查一般需要搭建实验环境进行升级规划的测试，测试对象包括规划中使用到的设备、协议、软件等，评估升级后的网络对原有网络性能的影响，获得的测试结果可以帮助修正升级规划，以便对其中不合理的部分进行调整，保证升级后的网络系统能够正常运行。

4. 升级的时间

升级的实施应在通过审查后进行，在升级前，应当预先对系统进行备份，以便在升级失败后能够恢复系统。升级应该按照计划严格执行，每完成一个阶段，就应该检查升级的结果并记录。

升级中常用到如下设备、工具和软件：

- 工作站和服务器
- 网络适配卡
- 集线器、路由器和交换机
- 测试设备
- 工作组和终端用户软件应用程序
- 数据交互方法
- 管理和控制应用程序(比如 SNMP，DHCP，DNS 和 NIS 等)

4.1.1.3 系统维护的高可靠性技术

1. 备件

在建设一个网络的同时，必须配备相应的备件。备件方式和备件策略的好坏直接影响到最终板件失效后的维修时间。备件离故障点越近，故障的维修时间就越短，网络的可用性就会越高，但是如果备件的库存太多又会增加库存的成本。需根据实际情况确定备件更换率、周转时间、备件成本等因素，综合分析确定备件策略。

2. 维护操作

维护操作失当是人为造成设备失效的主要原因，包括因操作流程的不规范和维护人员维护不及时等。

3. 服务水平

服务水平是体现设备商综合能力的重要因素，它直接影响到一个网络的可靠运营。对设备的定期巡检、对用户需求的快速响应、对设备问题的快速定位和及时处理、对客户的定期培训和交流等都会间接地提高网络的可用性。

4. 改进措施

针对备件、维护、服务等方面的常见改进措施如下：

(1) 优化维护体制，建立快速响应的维护队伍，减少业务中断时间。包括对设备的维修和传输介质的维修。

(2) 通过提高维护队伍的分布、技术水平，增加对维护人员的技术、流程培训，从而减少操作事故、减少故障定位时间。

(3) 制定完善的备件策略，减少备件响应时间。

(4) 采购设备时考虑设备制造商提供的服务水平。

(5) 增加计划性的维护，减少潜在故障的发生。

4.1.1.4 维护和升级的实施

1. 外部合同要点

网络维护和升级工作可由专门的网络维护服务公司来承担，他们的工作任务涵盖许多方面，除了制定相应的管理制度、提高计算机使用人员的素质外，还包括下面的一些具体工作：

(1) 建立技术档案

建立网络技术档案并为客户提供一份详细清单，包括应用软件的种类、名称、用途、版本号、开发商、参数设置等，以及网络的种类、拓扑结构、网络参数等。这些资料在维护工作中将起到重要的作用。

(2) 指导和培训

计算机软件使用指导和培训，包括协助用户进行应用软件的安装、调试，并协助解决使用中遇到的问题。指导用户更好地使用各类应用软件，避免因使用不当而导致的问题。

(3) 日常维护

日常网络维护是指定期上门为客户进行整个计算机网络的维护，现场监测系统的稳定性及运作状况，以保证整个系统正常运作。

(4) 紧急现场维护

紧急现场网络维护是指在用户遇到问题时及时上门排除故障。

(5) 重大时刻现场待命

重大时刻现场待命是指客户网络维护需要作重大调整或升级时，应该全程在场，随时待命，配合客户和供应商解决任何可能出现的问题。

2. 内部执行要点

网络管理人员需要完成的网络维护的工作内容如下：

(1) 病毒防治

病毒对网络系统危害很大，必须定期查杀，以免传播造成损失。

(2) 数据备份

数据备份是对网络操作系统、软件和数据的备份，它的目的是发生故障时恢复系统。

(3) 数据整理

定期整理计算机数据，清除无用的数据，修复错误的数据，维护系统的稳定性。

(4) 故障排除

发生故障时应及时发现并排除故障，以免造成更大的损失。

(5) 硬件维护

保持硬件清洁，有效保护硬盘、交换机等易损硬件，延长设备寿命。硬件出现故障时应及时维修。

(6) 指导培训

指导网络用户熟悉重要的操作规程，提高他们的操作能力。

4.1.1.5 系统容错技术

目前，计算机网络覆盖范围不断扩大，面临的新业务和用户也迅速增加，在网络运行过程中，随时都可能会出现各种意想不到的问题，其中很多问题可能会造成网络故障甚至导致网络的瘫痪，如不及时采取措施，将会给用户带来无法挽回的损失。因此，必须采用系统容错技术来解决。容错是指网络系统在出现错误(如硬件故障或用户误操作)的情况下仍能正常运转。

系统容错技术既可以采用硬件实现，也可以采用软件实现，还可以采取软硬件结合的系统容错方案来保证系统的可靠性。

常见的解决网络系统容错方案有 NEC 的容错服务器方案，NCR 公司的 Lifekeeper for NT，DIGTAL 公司的 NT Cluster，Fulltime 公司的 octopus 等等。下面简要介绍几种具有代表性的系统容错技术。

1. NEC 的容错服务器方案

顺应 IA 架构市场占有率的激增，以及 Windows 2000 Server 及 Linux 在服务器领域的迅猛发展潮流，NEC 公司通过与美国 Stratus 容错公司多年合作，于 2001 年推出了业界第一台基于 IA 架构、支持 Microsoft Windows 2000 Server 标准操作系统环境的容错服务器。它代表了 Microsoft Windows 平台上世界最高水平的系统可用性。该系列容错服务器采用 Intel 处理器及其他标准服务器部件，由于容错服务器的体系结构是属部件级冗余设计的体系结构，其结构的可靠度指标要比双机 Cluster 系统要高得多，以低成本实现了小型机的可靠性。

NEC 公司的 Express5800/ft 系列在 Windows 及 Linux 平台上的可靠性达到了 99.999%，代表了同等环境下全球最高的系统可用性。这种实时保护技术的来源是 Stratus 连续处理技术(Fundamentals of Continuous Processing Design)，它包括步锁(Lockstep)技术、安全故障(Failsafe)软件和激活服务(Active Service)结构 3 个基础。

2. Windows NT 的容错解决方案

NCR 公司是一家有着悠久历史的世界知名计算机厂商，在包括高可用性平台产品、电子商业、NT 企业服务器容错等七大尖端技术领域全球市场占有率第一。Lifekeeper for NT 软件是 NCR 公司推出的全球第一套基于 NT 操作系统的集群容错软件。Lifekeeper 系列产

品在我国金融、邮电、民航、证券等领域已取得广泛的应用，有力地促进了市场经济的发展。

Lifekeeper 是一套完善的实时容错软件，对硬件、操作系统、应用软件、业务数据均具备强大的容错性能。有些公司也推出自己的数据热备份软件，但这些软件只是做到了数据级备份，而对应用软件(如 SQL Server，Sybase 等)、系统软件(如 Windows NT)、系统硬件(如硬盘、内存、网卡)的容错却无能为力。一旦主服务器出现故障，正常业务将被迫终止且不能在短时间内恢复。

Lifekeeper 正是为满足这一社会需求而适时推出的容错软件，为关键业务的运行提供了保障。它是一个设计良好的集群容错软件，主要表现在：

- 能在主服务器发生技术故障时全自动地实现用户端应用系统以及服务器系统的热切换，真正实现用户端的应用连续性。
- 对备份服务器的硬件配置无任何特殊要求，用户可充分利用其原有的设备，从而大大节省投资。
- 既可支持共享磁盘阵列方式，又能支持纯软件容错的扩展方式，性能稳定可靠，能够给予客户在投入、连接结构等方面充分的选择余地。
- 能够做到同时支持 SQL Server，Sybase，Informix，Oracle，Notes，Exchange，SAP 等多种应用平台的灾难恢复。
- 对 NT，SQL 等数据库平台、硬件、应用软件的任何故障都能分别实现实时侦测，具备周全的容错切换机制。

系统容错技术的应用已经开始从过去的银行业、证券业、电信业等领域进入基础行业，如制造、能源、物流、交通，以及有着 7×24 小时不间断运营需求的中小商业团体和政府。系统容错技术的未来将会向着更高的可用性、更卓越的可维护性方向发展。

4.1.1.6　存储、备份与数据恢复

1. 网络数据存储

数据存储备份技术和存储管理技术源于 20 世纪 70 年代的终端/主机计算模式，由于数据主要集中在主机上，因此，管理方便的海量存储设备——磁带库是当时必备的存储设备。20 世纪 80 年代以后，由于 PC 技术的发展，尤其是 20 世纪 90 年代客户机/服务器模式的普及，数据的分布式存储加剧了数据存储管理的复杂化。

Internet 正在使存储技术发生着革命性的变化。这种变化主要表现在三个方面：首先是存储容量的急剧膨胀；其次是数据就绪时间的延长(网络数据必须保证全天候处于就绪状态)；最后，数据存储结构发生巨大变化。在 Internet 和全球化电子商务的时代，数据应该是面向全世界的，数据的存取只应该受到安全机制的限制，而不应该受到地域空间的约束。

网络环境中破坏数据的因素主要有以下几个方面：

- 自然灾害(如水灾、火灾、雷击、地震等)造成计算机系统的破坏，导致存储数据被破坏或完全丢失。
- 系统管理员及维护人员的误操作。
- 计算机设备故障，其中包括存储介质的老化、失效。

- 病毒感染造成的数据破坏。
- Internet 上“黑客”的侵入和来自内部网的蓄意破坏。

计算机系统不是永远可靠的，双机热备份、磁盘阵列、磁盘镜像、数据库软件的自动复制等功能均不能称为完整的数据存储备份系统，它们解决的只是系统可用性的问题，而网络系统的可靠性问题需要完整的数据存储管理系统来解决。所以说，网络设计方案中如果没有相应的数据存储备份解决方案，就不算是完整的网络系统方案。

目前市场上的存储产品主要有磁盘阵列、磁带机与磁带库、光盘库等，其中磁带设备以其技术成熟、价格低廉、产品齐全、使用方便等优点占据了存储市场的重要地位。

(1) 磁盘阵列

磁盘阵列又叫 RAID(Redundant Array of Inexpensive Disks，廉价磁盘冗余阵列)，是指将多个类型、容量、接口一致的专用硬盘连成一个阵列，使其能以某种快速、准确和安全的方式读写数据，从而提高数据存取速度和安全性。因此，磁盘阵列读写方式的基本要求是，在尽可能提高磁盘数据读写速度的前提下，必须确保在一张或多张磁盘失效时，阵列能够有效地防止数据丢失。磁盘阵列的最大特点是数据存取速度特别快，并将数据有选择性地分布在多个磁盘上，从而提高系统的数据吞吐率。另外，磁盘阵列还能够免除单块硬盘故障所带来的灾难后果，通过把多个较小容量的硬盘连在智能控制器上，增加系统存储容量。因此，磁盘阵列是一种高效、快速、易用的网络存储备份设备。

(2) 磁带库

磁带库产品包括自动加载磁带机和磁带库，它们实际上是将磁带和磁带机有机结合组成的。

自动加载磁带机是一个位于单机中的磁带驱动器和自动磁带更换装置，它可以从装有多盘磁带的磁带匣中拾取磁带并放入驱动器中，或执行相反的过程。它可以备份 100GB~200GB 或者更多的数据。自动加载磁带机能够支持例行备份过程，自动为每日的备份工作装载新的磁带。

磁带库是与自动加载磁带机类似的基于磁带的备份系统，它能够提供基本相似的自动备份和数据恢复功能，但同时具有更先进的技术特点。它的存储容量可达到数百 PB($1PB=10^6GB$)，可以实现连续备份、自动搜索磁带，也可以在驱动管理软件控制下实现智能恢复、实时监控和统计，整个数据存储备份过程无需人工干涉。磁带库不仅数据存储量较大，而且在备份效率和人工占用方面拥有无可匹敌的优势。在网络系统中，磁带库通过 SAN(Storage Area Network，存储局域网络)系统可形成网络存储系统，提供远程数据访问、数据存储备份，或通过磁带镜像技术实现多磁带库备份，为企业存储提供有力保障，无疑是数据仓库、ERP 等大型网络应用的良好存储设备。

(3) 光盘塔、光盘库和光盘网络镜像服务器

光盘塔由几台或十几台 CD-ROM 驱动器并联构成，可通过软件来控制某台光驱的读写操作。光盘塔可以同时支持几十个到几百个用户访问信息。

光盘库实际上是一种可存放几十张或几百张光盘并带有机械臂和一个光盘驱动器的光盘柜。它的库容量极大，机柜中可放几十片甚至上百片光盘片，这种有巨大联机容量的设备非常适用于图书馆一类的信息检索中心，尤其是交互式光盘系统、数字化图书馆系统、实时资料档案中心系统、卡拉 OK 自动点播系统等。光盘库的特点是：安装简单、使用方

便，并支持几乎所有的常见网络操作系统及各种常用通信协议，维护更换与管理非常容易，同时具有较低的成本和价格。又因光盘库普遍内置有高性能处理器、高速缓存器、快速闪存、动态存取内存、网络控制器等智能部件，使得其信息处理能力更强。

光盘网络镜像服务器是继第一代的光盘库和第二代的光盘塔之后，最新开发出的一种可在网络上实现光盘信息共享的网络存储设备。光盘网络镜像服务器不仅具有大型光盘库的超大存储容量，而且还具有与硬盘相同的访问速度，其单位存储成本(分摊到每张光盘上的设备成本)大大低于光盘库和光盘塔，因此光盘网络镜像服务器已开始取代光盘库和光盘塔，逐渐成为光盘网络共享设备中的主流产品。

在网络海量存储备份系统中，磁盘阵列、磁带库、光盘库等存储设备因其信息存储特点的不同，应用环境也有较大区别。磁盘阵列主要用于网络系统中的海量数据的即时存取；磁带库更多的是用于网络系统中的海量数据的定期备份；光盘库则主要用于网络系统中的海量数据的访问。

2. 网络备份

网络备份的最终目的是保障网络系统的顺利运行，所以一份优秀的网络备份方案应能够备份系统所有数据，在网络出现故障甚至损坏时，能够迅速地恢复网络系统和数据，将系统损失降到最低。

为了在整个网络系统内实现全自动的数据存储管理，必须安装网络数据存储管理系统，它能将备份服务器、备份管理软件与智能存储设备等有机地结合。另外，备份系统必须适应系统容量不断增加的要求，并且必须能够支持多平台系统和远程备份操作。

网络数据存储管理系统是指在分布式网络环境下，通过专业的数据存储管理软件，结合相应的硬件和存储设备，来对整个网络的数据备份进行集中管理，从而实现自动化地备份、文件归档、数据分级存储以及灾难恢复等。

网络数据存储管理系统的工作原理是在网络上选择一台应用服务器(当然也可以在网络中另配一台服务器作为专用的备份服务器)作为网络数据存储管理服务器，安装网络数据存储管理服务器端软件，作为整个网络的备份服务器。在备份服务器上连接一台大容量存储设备(磁带机或磁带库)。在网络中其他需要进行数据备份管理的服务器上安装备份客户端软件，通过局域网将数据集中备份到与备份服务器连接的存储设备上。

网络数据存储管理系统的核心是备份管理软件，通过备份软件的计划功能，可为整个企业建立一个完善的备份计划及策略，并可借助备份时的呼叫功能，让所有的服务器备份都能在同一时间进行。备份软件也提供完善的灾难恢复手段，能够将备份硬件的优良特性完全发挥出来，使备份和灾难恢复时间大大缩短，实现网络数据备份的全自动智能化管理。

数据备份的方式有多种，下面以磁带机为例，简述全备份、增量备份和差分备份的区别和应用。

(1) 全备份

全备份(Full Backup)就是对整个系统进行完全备份，包括系统和数据。这种备份方式的最大优点是操作比较简单，当发生数据丢失时，只要用一盘磁带就可以完全恢复系统和数据。然而它也有缺点：首先在备份数据中有很多重复数据存在，它们占用大量的磁带空间，增加了应用系统的运行成本；其次，备份数据量大，备份时间长。不适用于那些业务繁忙，备份时间有限的场合。

(2) 增量备份

增量备份(Incremental Backup)就是每次只对上一次备份后增加的和修改过的数据进行备份。这种备份的优点很明显：没有重复的备份数据，既节省磁带空间，又缩短了备份时间。但它的缺点在于当发生灾难时，恢复数据比较麻烦；另外这种备份可靠性也差。在这种备份方式下，各磁带间相互关联，其中任何一盘磁带出了问题都不能完全恢复系统。

(3) 差分备份

差分备份(Differential Backup)就是对上一次全备份之后新增加的和修改过的数据进行备份。它需要与全备份配合使用，例如，管理员先在星期一进行一次系统完全备份；然后在接下来的几天里，管理员再将当天所有与星期一不同的数据(新的或经改动的)备份到磁带上。

(4) 三种备份方案的比较

由上述可以看出，全备份所需时间最长，但恢复时间最短、操作最方便，当系统中数据量不大时，采用全备份最可靠；差分备份在避免了另外两种策略缺陷的同时，又具有了它们的所有优点。首先，它无需每天都做系统完全备份，因此备份所需时间短，并节省磁带空间；其次，它的灾难恢复也很方便，系统管理员只需两盘磁带，即星期一的磁带与发生灾难前一天的磁带，就可以将系统完全恢复。在备份时要根据它们各自的特点灵活使用。

3. 灾难恢复

灾难恢复的先决条件是要作好备份策略及恢复计划。日常备份制度描述了每天的备份以什么方式、使用什么备份介质进行，是系统备份方案的具体实施细则。在制定完毕后，应严格按照制度进行日常备份，否则将无法恢复系统。

灾难恢复措施在整个备份制度中占有相当重要的地位。因为它关系到系统、软件与数据在经历灾难后能否迅速恢复如初。全盘恢复一般应用在服务器发生意外灾难导致数据全部丢失、系统崩溃或是有计划地系统升级、系统重组等时，也称为系统恢复。

一个完整的灾难备份及恢复方案，包括备份硬件、备份软件、备份制度和灾难恢复计划四个部分。若想做到数据的万无一失，还需要根据企业自身情况制定日常备份制度和灾难恢复措施，并由管理人员切实执行备份制度，否则数据安全将是空谈。

4.1.1.7 网络系统的配置管理

配置管理的目的在于维护及优化网络，其功能是对网络的组件进行识别、定义、控制和监视，实现网络的某些特定功能并使网络性能达到最优。网络系统时刻处于变化之中，网络系统本身要随着用户的增减、系统应用项目变化及设备的维修或更新来及时调整网络的配置，使网络能更有效地工作。

网络配置包括配置节点和集中器数量、分布和互联情况、线路的数量和速率，以及设备的通信模板和端口个数等。配置管理可以视网络的规模和能力随需要而改变。一般包括以下内容：

- 网络资源的自动发现和图形化表示，以及网络资源的管理信息。
- 网络资源的对象化管理，被管对象和被管对象组的命名管理、初始化和关闭等。
- 软件及硬件资源与版本数据的管理。

- 设备端口状态。
- IP 地址资源分配与管理、网络 IP 地址与 MAC 地址对应及 IP 地址冲突检测。
- 子网及主机情况。
- 设备路由信息，系统中有关路由操作的参数配置。
- 系统配置信息，更改系统的配置。
- 配置及资产统计报告。

下面简要介绍设备管理、软件管理和网络配置图。

1. 设备管理

设备管理包括资产管理、设备变化的管理和设备配置管理等。

(1) 资产管理

资产管理是检验和跟踪网络上的软硬件。资产管理的第一步是为网络上的每一个节点列出清单，它不仅应包括网络上各种设备的总数，还应该包括每个设备的配置文件、型号、序列号、在网络上的位置以及技术支持的联络方式等。另外，还应该保留公司所购买的软件的记录、版本号、供应商、技术支持和联络方式等。

资产管理工具的选择应依公司需求而定，可以购买专用的资产管理软件，它们通常能够自动检测网络上所有设备并把相关信息保存到数据库中，也可以使用电子表格软件来存储资产数据。另外应该保证资产管理数据库信息随着网络软件和硬件的变化定期地更新(自动或手动)。

资产管理使网络管理和升级更加容易，简化网络管理员的工作。

(2) 设备变化的管理

作为系统管理员，应该时刻关注在网络正常运行或排障过程中的网络系统的改变，以及在管理和升级过程中的网络问题。设备变化的管理系统帮助将网络元件的移位或改变同网络的不同表现联系起来，简化了描绘基准线和测量网络性能的过程。同资产管理系统一样，变化管理系统也应该保持实时更新。但与资产管理不同的是，变化管理的记录不能由专用程序(能够自动发现网络硬件或软件的程序)生成，而必须由网络管理员提供变化发生的具体情况信息。

(3) 设备配置管理

配置管理为所有基于命令的或者基于 IOS 的交换机和路由器提供了一种访问配置的简单方法。一旦设备处于被管理状态，其配置文件将自动收集配置信息并存放在资源管理服务器上。通过临近系统的日志消息、SWIM 任务、检查设备清单的变化、安排轮询等可以做到自动更新配置文件。

配置管理的后台进程能够保证配置文件时刻更新。一旦配置文件生成后，管理员便可以对这些文件执行多种任务，常见的任务如下：

- 运行变化报表　找到配置文件的变化，列出变化细节并指明管理员的责任。
- 调试自动报表　无需时刻监督运行报表，便可以生成历史报表。
- 查询配置文件　按照特征串搜索配置文件或其他文件。
- 比较配置文件　找出两个配置文件的差别。
- 创建定义报表　基于配置文件中的文本串生成报表。

很多厂商的设备都提供了完备的配置管理工具，例如 Cisco 除了提供文件管理功能之

外，它的 Resource Manager 软件还提供了 NetConfig 工具，利用这个工具，可以对被管理的设备配置进行实时更改和查询。NetConfig 工具还允许管理员创建自定义的模板，它们是一些命令集，用于改变网络中的一个或多个设备，这些自定义的管理命令可以在路由器或交换机上执行。

2. 软件管理

为了保证系统中各种软件能够正常运行，需要对它们进行必要的管理，软件管理除了包括软件正常的维护外，还应包括软件系统的改变。网络上常见的软件改变如下：

- 补丁　对某一段程序的提高或加深。
- 升级　对已有代码的主要改变。
- 修订　对已有代码的部分改变。

通常所说的补丁是对软件特定部分的提高和加强，它区别于软件升级和修订，它只改变软件程序的一部分，不改动大部分的代码。补丁经常被用于修复代码中的错误(bug)，或者稍微地增加软件功能。补丁不是对整个软件包的替换，相反，补丁是安装在软件之上的，补丁也不仅仅限于网络操作系统软件，还可能针对其他很多软件。维护网络过程中会遇到管理网络各个不同部分的补丁，有时甚至需要补充服务器的操作系统。

尽管对每种类型的软件的改变不同，但是通常的改变步骤可归纳如下：

(1) 考虑改变(不论是补丁、升级还是修订)是否必要。
(2) 研究改变的目的和它对程序可能产生的影响。
(3) 考虑改变是适用于部分用户还是所有用户；应该集中执行还是逐步执行。
(4) 制定在非工作时间的改变进度(除非它是紧急的)并通知用户。
(5) 备份当前的系统或软件。
(6) 防止用户登录处于变动中的系统或部分系统(例如可以限制登录)。
(7) 执行改变(保证按照升级向导进行并记录修改)。
(8) 在改变之后测试整个系统，完整地测试软件并观察结果。
(9) 如果改变成功，则开放该系统并通知用户；否则应恢复旧版本。

网络管理人员应该根据软件提供商的建议升级和补丁软件，这样可以避免出现不必要的网络故障。

3. 网络配置图

网络配置图是一张网络主要设备的部署结构图，它包括网络系统中所有的主要设备、节点和线路，以及它们之间的连接方式和相对的位置关系。从网络配置图中可以获取许多关于网络系统较重要的信息，比如网络的拓扑结构、设备配置、传输能力、冗余度等，既便于了解网络配置状况，又有利于网络管理人员的日常维护工作。图 4.1 是一张典型的校园网络配置图。

在配置管理中，通常使用网络配置图将网络的配置用图形表示出来，包括每个组件的名称、IP 地址。对每个网段和广域通信连接，还要标上速率、使用的协议和子网地址。

格式规范的配置文档都应附有网络配置图。

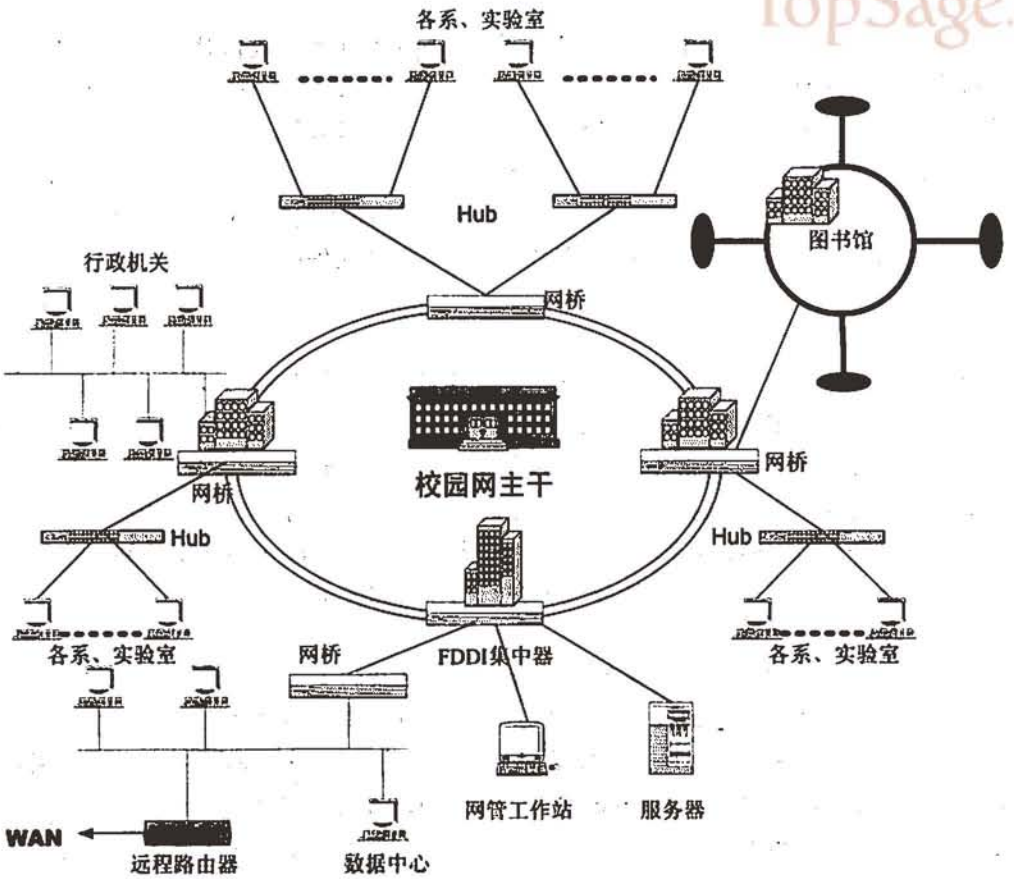


图 4.1 校园网络配置图示例

4.1.2 典型例题分析

例 1 根据工作经验，谈谈实施添加或升级网络设备的注意事项。

分析：在网络上添加或升级的每种设备都有不同的准备和安装要求。要确切知道怎样处理这些变化，不仅要仔细阅读生产商的手册，还要能获得一些这种设备的相关安装经验。

下面针对常见的网络设备提供一些建议：

(1) 网络工作站

网络工作站是所添加的最简单的设备，因为它只直接影响很少的用户，不改变其他用户访问网络的能力。如果有联网工作站的标准配置(如磁盘映像，即在服务器上对工作站内容压缩的快照)，增加一个网络工作站将会很快完成。

(2) 网络打印机

添加网络打印机比添加工作站稍微复杂一些，因为它需要单独配置操作而且它是共享的。尽管它影响多个用户，打印机在网络中不起关键作用，所以安装打印机并不会影响工作。

(3) 网络集线器

一个单独的集线器可以支持 4~64 个用户。但是在添加新集线器时不必担心停机时间或通知用户，在真正使用之前它不可能影响任何用户。如果打算升级或拆除一个集线器，必须通知受影响的用户，因为升级和拆除将造成死机，所以必须在非工作时间实施操作。另外，在添加和升级集线器时必须考虑流量和地址限制。例如，需要扩充基于 TCP/IP 协议的一段网络容量(从 24 个用户到 60 个用户)，用 64 口集线器代替 24 口集线器非常容易。在此之前，确保这一网段有足够的 IP 地址以为 60 个用户提供服务，否则，这些用户不能登录网络。

(4) 服务器

升级和添加一个服务器需要(除非它只是替换显示器)周密计划。在安装新服务器之前，不仅需要考虑与变化有关的硬件和连接设备，还要考虑和网络操作系统有关的问题。即使是打算添加一台暂时不用的服务器，也要计划它的安装，最好是在网络流量小的时候添加服务器。另外还要限制对服务器的登录，否则，用户可能会对其进行非法操作。升级已有服务器上的硬件(像网络接口卡和内存)需要像升级全新服务器一样仔细计划，应该在脱机状态下实施升级计划，这样升级任务就不会影响任何用户的工作。

(5) 交换机和路由器

添加、改变交换机和路由器是网络设计中最为复杂的工作。这是因为：首先，它们可能受到物理损坏，也就是它们经常要求在通信设备间安装新的配线架或其他支撑设备。其次，它们影响到许多用户，也许是所有的网络用户。例如，假如必须替换 Internet 网关，在此过程中必须切掉每个用户的 Internet 登录。即使网络上的用户不可能受到影响，也要通知他们。有时一个路由器和交换机可能导致故障，但不是在服务器的区段上，而是在另一网段上。另外，应该提前(至少在几周前)设计交换机和路由器的改变计划，预期至少几小时的死机时间。因为路由器和交换机是贵重设备，故在处理和配置设备时要格外小心。同样，因为交换机和路由器提供不同目的的服务，应依靠生产商的文档引导安装进程。

答案：在网络设备的安装和升级中，从简单的网络工作站、网络打印机、网络集线器的安装或升级，到较为复杂的服务器、交换机和路由器的安装和升级，都应该掌握一定的策略，这样才能保证添加设备后网络能够正常运转。

例 2 Windows 组网中采用什么工具来实现域的创建和管理？在什么情况下需要设置“主域”？(2003 年下午试题四问题 3)

分析：

PDC(主域控制器)是在 Windows NT Server 4.0 域或更早的域中，运行 Windows NT Server 并对域登录进行身份验证的计算机，该计算机也用来维护域的目录数据库，PDC 跟踪对域中所有计算机账户所做的更改。它是直接接收这些变化的惟一计算机，每个域只有一个 PDC。

答案：通过 PDC(主域控制器)工具来实现域的创建和管理，该进程运行在 Windows NT Server 上。主域被其他域信任，但主域不信任其他域。当有些部门要单独控制它们拥有的资源，但又要求保持集中身份验证时，需要设置主域。

例 3　某公司规模扩大，既要考虑保证目前土建装修的效果不被破坏，又要满足网络扩容和企业工作实际需求，同时还要保证投资不要过大。请为该公司设计网络升级方案。

分析：公司的规模扩大，需要对现有网络进行改造升级，但又不能破坏当前的建筑布局，传统的网络布线(铺设光纤、双绞线等)都必须挖沟开槽，势必破坏该公司的土建装修的效果，不满足要求，故必须考虑采用其他组网技术。无线局域网 WLAN 是最佳选择，因为它不需要铺设线缆，只需要安装有限个接入点(AP)就可支持一定范围内的无线接入服务。

在一个典型的 WLAN 环境中，有一些进行数据发送和接收的设备，称为接入点(AP)。通常，一个 AP 能够在 30m~100m 的范围内连接多个无线用户。在同时具有有线和无线网络的情况下，AP 可以通过标准的 Ethernet 电缆与传统的有线网络相连，作为无线网络和有线网络的连接点。WLAN 的终端用户可通过无线网卡访问网络。

因此，采用 WLAN 方案可以满足该公司要求，并将新的 WLAN 与旧有的局域网连接起来。另外，这种方案的投资也较节省。

答案：经过深入分析和研究对比，建议采用无线局域网 WLAN 组网方案来解决网络扩容的问题。

4.1.3　同步练习

1. 网络升级的原则是什么？
2. 网络升级的要求有哪些？
3. Linux 系统中怎样进行用户管理？
4. 网络存储备份系统的设计目标是什么？
5. 什么是基准线？它在网络的维护过程中有何作用？

4.1.4　同步练习参考答案

1. 由于网络升级工作牵涉到很多因素，因此在制定网络升级计划时必须遵循一些基本的原则，并且要明确网络升级的目的，以免产生偏差。升级原则如下：

- 最大限度地保护已有投资。
- 采用成熟的主流技术。
- 实用性与先进性相结合。
- 综合分析、全面考虑网络升级内容。

2. 网络升级的主要目的是提高网络性能，满足网络应用的需求。一般来说，通过网络升级，就能够使网络在以下几个方面得到改善：

- 高速率和稳定性。
- 提高网络的可靠性。
- 增加网络系统的安全性。
- 增强系统的能力。
- 易管理性。
- 无故障升级。

3. Red hat Linux 是一个多用户系统，当一台计算机多人使用时，通常需要区分用户，因此每个用户需要一个单独的用户名用于登录。另外单个用户也可以作为用户组的成员。在 Linux 中用户管理的方法有多种，包括行命令方式、手工方式和图形界面方式等，每种方法各有优缺点。

(1) 系统管理员

系统管理员是特殊的用户，通常一般用户只管运行个人的应用程序，属于系统支持方面的工作，则由系统管理员来负责。系统管理员有一个专用账户即 root，登录时输入：

```
$ login root
Password:******
#
```

以 root 用户名并输入管理员口令即可登录系统，此时用户身份是管理员。也可以使用替换用户命令 su 登录管理员环境。

(2) 用户管理

用户管理中主要包括以下一些操作：

① 添加用户。添加用户使用 useradd 命令，该命令选项较多，如不指定则按默认方式处理。useradd 并不为用户设置口令，必须使用 passwd 命令进行口令设置后，该用户才可以正式使用。

② 设置口令。建立一个新用户后必须为其设置口令，设置口令的命令是 passwd，系统管理员可以使用该命令为普通用户设置口令，命令格式如下：

```
passwd [-u] [username]
```

③ 删除用户。使用 userdel 命令删除用户，命令格式如下：

```
userdel [-r] [username]
```

(3) 用户组管理

① 添加用户组。使用 groupadd 命令添加用户组，格式如下：

```
groupadd [-g gid[-o]] [-r] [-f] [group]
```

② 删除用户组。使用 groupdel 命令删除用户组。格式如下：

```
groupdel [group]
```

③ 修改用户组属性。使用 groupmod 命令修改用户组属性。格式如下：

```
groupmod [-g gid[-o]] [-n group_name][group]
```

另外，还可以使用 LinuxConf 图形工具管理用户和用户组。

4. 理想的网络存储备份系统设计应该提供多层的服务。应该提供如下功能：

- 集中式管理
- 数据库备份和恢复、全自动备份
- 提供在线式索引
- 归档管理
- 存储介质管理

- 分级存储管理
- 系统灾难恢复
- 满足系统不断增加的需求

5. 正确维护网络的第一步是标记它当前的状态。只有分析了网络过去的性能之后，才能预测网络将来的状态。测量和记录网络当前状态的操作叫标定基准线(base lining)。基准线参数包括主干网的利用率，每日、每小时登录的用户数，网络上运行的协议数，错误的统计数(例如：巨型包、冲突、坏的部件，或者是碎包等)，网络设备被使用的频率，或者有关哪个用户占用了最多带宽的信息等。

正确掌握网络的基准线，有利于确定正常运行的状态，对快速判断异常情况有很大帮助。

4.2 本 章 小 结

本章主要介绍了网络系统的运行和维护内容。网络维护是保障网络正常运行的重要方面，主要包括故障检测与排除、网络日常检查及网络升级。其中较为重要的工作是用户管理、可靠性措施的设计和实施，做好系统重要数据和应用程序的备份和恢复工作，合理配置网络，并在系统老化过程中有计划有步骤地进行网络升级，需要着重掌握。

第 5 章　网络系统的管理

大纲要求：

- 网络系统的监视　网络管理协议(SNMP、MIB-Ⅱ、RMON)，利用工具监视网络性能，利用工具监视网络故障，利用工具监视网络安全(入侵检测系统)，性能监视的检查点，安全监视的检查点。
- 故障恢复分析　故障分析要点，排除故障要点，故障报告撰写要点。
- 系统性能分析　系统性能分析任务。
- 危害安全的对策　危害安全情况分析(调查损失情况、收集安全信息、查找原因)，入侵检测要点，对付计算机病毒的要点(查杀病毒措施)。

5.1　网络系统的监视

5.1.1　考点辅导

5.1.1.1　网络管理功能

在 OSI 系统管理标准中，将开放系统的管理功能划分为 5 个功能领域，它们是：配置管理、性能管理、故障管理、安全管理和计费管理功能领域。这 5 个功能领域覆盖了网络管理所需的主要功能，为网络管理系统功能分析、设计和实现提供了基本概念。

1. 配置管理

配置管理是最基本的网络管理功能，负责监测和控制网络的配置状态。具体地讲，就是在网络建立、扩充、改造以及业务的开展过程中，对网络的拓扑结构、资源配备、使用状态等配置信息进行定义、监测和修改。

2. 性能管理

性能管理保证有效地运营网络并提供约定的服务质量。在保证各种业务的服务质量(QoS)的同时，尽量提高网络资源利用率。性能管理包括性能监测功能、性能分析功能和性能管理控制功能。

3. 故障管理

故障管理的作用是迅速发现和纠正网络故障，动态维护网络的有效性。故障管理的主要功能有报警监测、故障定位、测试、业务恢复以及修复等，同时还要维护故障日志。

4. 安全管理

安全管理的作用是提供信息的保密、认证和完整性保护机制，使网络中的服务、数据和系统免受侵扰和破坏。安全管理主要包含风险分析功能，安全服务功能，告警、日志和报告功能以及网络管理系统保护功能。

5. 计费管理

计费管理的作用是正确地计算和收取用户使用网络服务的费用，进行网络资源利用率的统计和网络的成本效益核算。计费管理主要提供费率管理功能和账单管理功能。

5.1.1.2　网管系统的构成

一个完整的网络管理系统由多个部件组成，主要包括：

- 网络管理协议
- 网络管理工作站
- 被管网络部件
- 管理信息库 MIB

作为管理者(manager)，一个网络系统中可以有一个(或者几个)网络管理工作站；被管理者称作代理(agent)，网上具有多个被管网络部件；网络管理协议是管理者和被管理者之间的操作规范，而具体的操作对象则是管理信息的集合——管理信息库(Management Information Base，MIB)。

网络管理系统的基本工作流程为：

(1) 在被管理部件上预置代理。

(2) 网络管理者使用网络管理协议从代理的 MIB 中取得被管网络部件的管理信息，并存入自己的 MIB。

(3) 管理软件通过对 MIB 的分析处理，达到网络监控管理目的。

5.1.1.3　网络管理协议

网络管理协议是管理者和被管理者之间共同遵循的规则，它们之间可以通过网络管理协议完成管理信息的交换任务。常用的网络管理协议包括：SNMP、MIB-II 和 RMON 等，它们都基于 TCP/IP 协议工作。

1. SNMP

(1) SNMP 概述

SNMP 的前身是简单网关监控协议(SGMP)，用来对通信线路进行管理。随后对其改进并加入了符合 Internet 定义的 SMI 和 MIB 体系结构，改进后的协议就是著名的 SNMP。SNMP 的目标是管理 Internet 上众多厂家生产的软硬件平台，因此 SNMP 受 Internet 标准网络管理框架的影响也很大。SNMP 的体系结构如图 5.1 所示。

SNMP 的体系结构围绕以下 4 个概念和目标进行设计：

- 使管理代理(agent)的软件成本尽可能低。
- 最大限度地保持远程管理的功能，以便充分利用 Internet 的网络资源。
- 体系结构必须有扩充的余地。
- 保持 SNMP 的独立性，不依赖于具体的计算机、网关和网络传输协议。

在 SNMP 改进版本 SNMPv2 中，又加入了保证 SNMP 体系本身安全性的目标。

另外，SNMP 中提供了 4 类管理操作：

- get 操作　用来提取特定的网络管理信息。

- get-next 操作　通过遍历操作来提供强大的管理信息的提取能力。
- set 操作　用来对管理信息进行控制(修改、设置)。
- trap 操作　用来报告重要的事件。

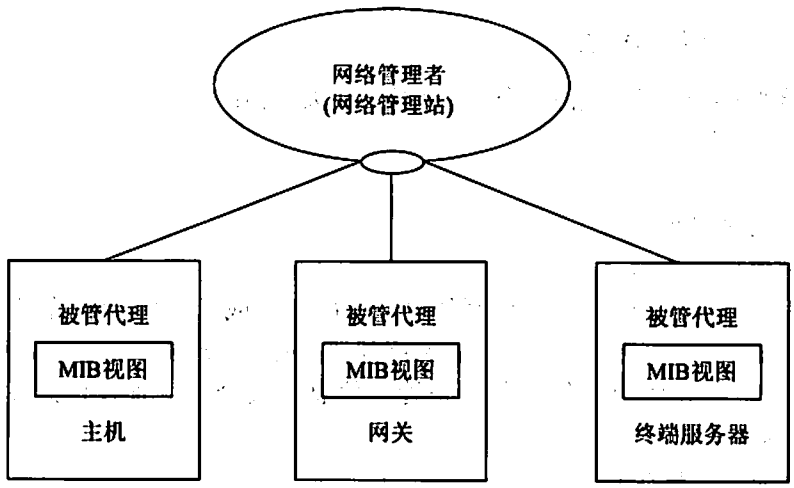


图 5.1　SNMP 的体系结构

各种操作的执行如图 5.2 所示。

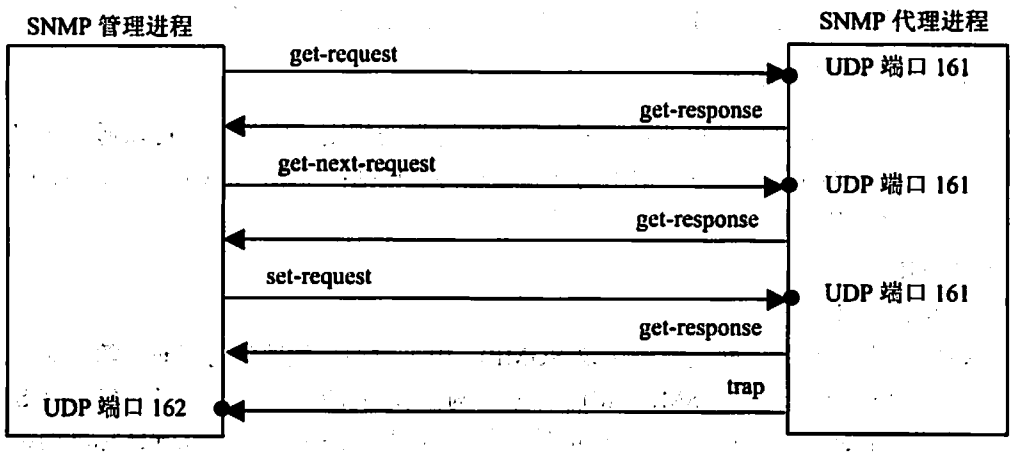


图 5.2　SNMP 的 4 种操作

(2) SNMP 管理控制框架与实现

① SNMP 管理控制框架

SNMP 定义了管理进程(manager)和管理代理(agent)之间的关系，这个关系称为共同体(community)。描述共同体的语义是非常复杂的，但其句法却很简单。位于网络管理工作站(运行管理进程)上和各网络元素上，利用 SNMP 相互通信，并对网络进行管理的软件统称为 SNMP 应用实体。若干个应用实体和 SNMP 组合起来形成一个共同体，不同的共同体之间用名字来区分，共同体的名字必须符合 Internet 的层次结构命名规则，由非保留字符串组成。此外，一个 SNMP 应用实体可以加入多个共同体。

SNMP 的应用实体对 Internet 管理信息库中的管理对象进行操作。一个 SNMP 应用实

体可操作的管理对象子集称为 SNMP MIB 授权范围。SNMP 应用实体对授权范围内管理对象的访问还有进一步的访问控制限制，比如只读、读/写等；SNMP 体系结构中要求每个共同体都规定其授权范围及其对每个对象的访问方式。记录这些定义的文件称为共同体定义文件。

SNMP 的报文总是源自每个应用实体，报文中包括该应用实体所在的共同体的名字。这种报文在 SNMP 中称为有身份标识的报文，共同体名字是在管理进程和管理代理之间交换管理信息报文时使用的。管理信息报文中包括以下两部分内容：

- 共同体名　加上发送方的一些标识信息(附加信息)，用以验证发送方确实是共同体中的成员，共同体实际上就是用来实现管理应用实体之间身份鉴别的机制。
- 数据　这是两个管理应用实体之间真正需要交换的信息。

在第三版本前的 SNMP 中只是实现了简单的身份鉴别，接收方仅凭共同体名来判定收发双方是否在同一个共同体中，而前面提到的附加信息尚未应用。接收方在验明发送报文的管理代理或管理进程的身份后要对其访问权限进行检查。访问权限检查涉及到以下因素：

- 一个共同体内各成员可以对哪些对象进行读、写等管理操作，这些可读写对象称为该共同体的授权对象(在授权范围内)。
- 共同体成员对授权范围内每个对象定义了访问模式：只读或可读写。
- 规定授权范围内每个管理对象(类)可进行的操作(包括 get，get-next，set 和 trap)。
- 管理信息库(MIB)限制对每个对象的访问方式 (如 MIB 中可以规定哪些对象只能读而不能写等)。

管理代理通过上述预先定义的访问模式和权限，来决定共同体中其他成员要求的管理对象访问(操作)是否允许。共同体概念同样适用于转换代理(proxy agent)，只不过转换代理中包含的对象主要是其他设备的内容。

② SNMP 实现方式

为了提供遍历管理信息库的手段，SNMP 在其 MIB 中采用了树状命名方法对每个管理对象实例命名。每个对象实例的名字都由对象类名字加上一个后缀构成，对象类的字是不会相互重复的，因而不同对象类的对象实例之间也很少有重名的危险。

在共同体的定义中一般要规定该共同体授权的管理对象范围，相应地也就规定了哪些对象实例是该共同体的“管辖范围”，据此，共同体的定义可以想像为一个多叉树，以词典序提供了遍历所有管理对象实例的手段。有了这个手段，SNMP 就可以使用 get-next 操作符，顺序地从一个对象找到下一个对象。get-next(object-instance)操作返回的结果是一个对象实例标识符及其相关信息，该对象实例在上面的多叉树中紧排在指定标识符 object-instance 对象的后面。这种手段的优点在于，即使不知道管理对象实例的具体名字，管理系统也能逐个地找到它，并提取到它的有关信息。遍历所有管理对象的过程可以从第一个对象实例开始(这个实例一定要给出)，然后逐次使用 get-next，直到返回一个差错(表示不存在的管理对象实例)结束(完成遍历)。

由于信息是以表格形式(一种数据结构)存放的，在 SNMP 的管理概念中，把所有表格都视为子树，其中一张表格(及其名字)是相应子树的根节点，每个列是根下面的子节点，一列中的每个行则是该列节点下面的子节点，并且是子树的叶节点，如图 5.3 所示。

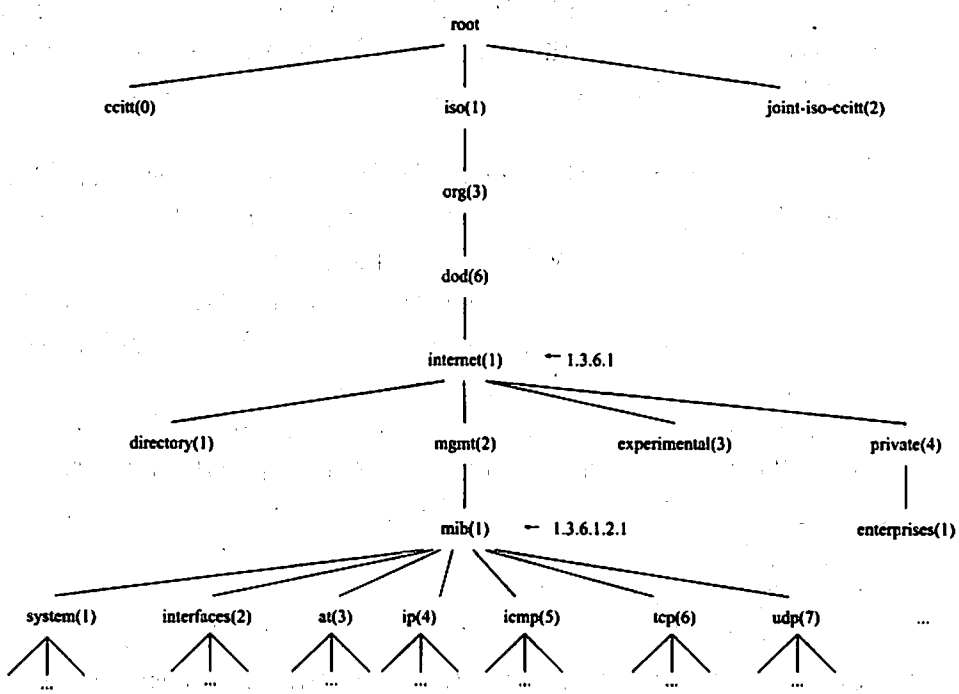


图 5.3 管理信息库中的对象标识

因此，按照前面的子树遍历思路，对表格的遍历是先访问第一列的所有元素，再访问第二列的所有元素……直到最后一个元素。若试图得到最后一个元素的“下一个”元素，则返回差错标记。

SNMP 中各种管理信息大多以表格形式存在，一个表格对应一个对象类，每个元素对应于该类的一个对象实例。那么，管理信息表对象中单个元素(对象实例)的操作可以用前面提到的 get-next 方法，也可以用 get/set 等操作。下面主要介绍表格内一行信息的整体操作。

- 增加一行 通过 SNMP 只用一次 set 操作就可在一个表格中增加一行。操作中的每个变量都对应于待增加行中的一个列元素，包括对象实例标识符。
- 删除一行 删除一行也可以通过 SNMP 调用 set 操作将该行中的任意一个元素(对象实例)设置成“非法”即可。

至于删除一行时，表中的一行元素是否真的在表中消失，则与每个设备(管理代理)的具体实现有关，因此管理进程必须能通过各数据字段的内容来判断数据的合法性。

(3) SNMP 协议

SNMP 是一个异步的请求/响应协议，即 SNMP 的请求和响应之间没有必定的时间顺序关系，换句话说，SNMP 是一个面向无连接的协议。这样，SNMP 实体不需要在发出请求后立即等待响应的到来，因此 SNMP 响应也可能丢失或出现错误。

SNMP 中设计了四种基本协议交互过程。

第一种情况是管理进程从管理代理处提取管理信息：管理进程通过 SNMP 和传输网络发送 get-request 给管理代理，请求中包括管理对象的标识符等参数；管理代理收到请求后

返回相应内容的 get-response，响应中包括待提取的管理信息。

第二种情况是管理进程在管理代理的可见范围内遍历一部分管理对象实例：管理进程通过 SNMP 和传输网络发送 get-next-request 给管理代理，管理代理收到后完成遍历的一次操作，用 get-response 将遍历结果返回给管理进程。

第三种情况是管理进程在管理代理中存储信息，即对管理代理的管理信息库 MIB 进行写操作(包括设置工作参数)：管理进程发送一个 set-request 给管理代理，由管理代理完成 set 操作，然后用 set-response 返回操作结果。

第四种情况则是管理代理主动向管理进程报告事件：管理代理通过 SNMP 和传输网络将 trap 发送给管理进程，这个操作没有响应。

注意，上面的各个请求都是管理进程发给管理代理的，响应则都是由管理代理发给管理进程的。只有 trap 是无响应的，由管理代理单向发给管理进程。另外，请求、响应和 trap 的传输处理都要受“共同体”定义的限制，包括访问权限。

SNMP 协议是一个对称协议，没有主从关系。SNMP 上的管理进程和管理代理都可以得到 SNMP 完全相同的服务。下面对 SNMP 协议的部分特点和关键内容进行介绍。

① 管理信息报文

在大多数 SNMP 操作中都使用一个相同的报文数据结构。对于前面提到的身份鉴别方法，报文中包含三种数据(信息)传递给专门的“身份鉴别实体”：共同体名称、有关数据和发送方 SNMP 实体的传输层地址。

身份鉴别实体负责验证发送方是否是合法的对等实体，并返回两种可能的结果：一种结果是返回本次报文中的 SNMP 协议数据类型和发送方 SNMP 实体的权限标识符；另一处结果是返回例外。其中第一种结果表明发送方 SNMP 实体确实是本共同体的成员之一，接收方 SNMP 实体接下来对它进行处理。第二种结果(“例外”)表明发送方 SNMP 实体并非本共同体成员，不能接受此报文，并且接收方 SNMP 实体还可能根据配置产生一个“身份非法”的 trap 事件。

② 协议数据单元及其管理操作

SNMP 协议实体之间的协议数据单元(PDU)只有两种不同的结构和格式，一个 PDU 格式在大部分操作中使用，而另一个则只在 trap 操作中作为 trap 的协议数据单元。

PDU 一般包含多个代表特殊意义的字段：request-id 是一个整数值，用来区分不同的 PDU，error-status 反映管理操作是成功还是失败；error-index 表明操作中哪个变量错误，variable-bindings 是一系列变量的清单，序列中每一项包含一个变量名及其变量值。

在 SNMP 中，接收方完成身份鉴别并得到共同体定义信息之后，SNMP 实体根据 PDU 内容执行几种操作：get 操作，根据变量名取出指定的对象实例；get-next 操作，该操作与 get 操作不同，不是取变量名指定的对象实例，而是取出变量名指定的对象实例的按词典排序的下一个对象实例；set 操作，对指定对象实体的值用请求中的新值替换；get-response 对 get/set 报文做出响应并返回操作结果，收到该响应报文的操作请求方首先根据报文中的 request-id 在记录中查找有无这个序号的请求，如果没有，则丢弃该响应，否则接收该响应，管理进程要进行响应处理。

③ trap 操作

trap 是一种捕捉事件并报告的操作，实际上几乎所有网络管理系统和管理协议都具有

这种机制。在OSI网络管理国际标准中称为“事件和通报”，一般都简称为事件报告。

为了减少管理信息业务流量，管理代理负责对管理对象的trap进行检查，管理检查可以设置检查条件，这样，管理进程就可以在一定程度上控制trap报告过程。引入trap报告的最大好处是许多重要事件的发生得以及时让管理进程知道。因为一般只有比较关键的trap事件才确实需要报告，再加上每个trap事件都很简短，因此由于trap而引入的不确定管理信息业务量是较少的，但却能大大改善网络管理的时效性。

由于事件多种多样，各种事件发生环境也很不一样，trap操作的复杂性比前面讲的几种操作都大，SNMP的trap操作PDU中字段类型也较多。这些trap操作PDU中的字段包括：enterprise，记录发送trap事件的管理代理的标识符；agent-addr，管理代理的网络节点地址；generic-trap，描述该trap操作报告是哪一种异常事件；specific-trap，给出各管理代理自行定义的trap事件代码；time-stam，表示trap事件发生的时刻；variable-bindings，这个字段给出一组变量，这些变量及其值给出了与trap事件有关的详细信息。

当管理代理检测到一个例外或异常事件发生时，管理代理首先要判断需要将该事件报告给哪个或哪些管理进程。对每个管理进程，管理代理要选择相应的共同体号，由SNMP协议实体按照前面的字段格式构造trap报告PDU发送出去。

④ SNMP PDU的传输

SNMP的设计是独立于具体的传输网络的，也就是说，它既可以在TCP/IP的支持下操作，也可以在OSI的传输层协议支持下完成操作，甚至可以在以太网的直接支持下实现操作。其中对OSI传输层服务没有要求，既可以是有连接的服务，也可以是无连接的服务。为了实现上述目标，Internet组织定义了若干映射标准，规定了如何将SNMP协议数据单元PDU映射到下层的无连接传输请求上去。

所有各种映射定义中，有一点是相同的，即所有SNMP报文数据是通过一个“顺序化”过程在网络上传输的，这个顺序化过程可以将任意结构的数据编码成一个有序的字符串进行传送。收到这些字符串后则按照完全相同的语法将它们解码成原来的数据结构。

⑤ MIB中为SNMP定义的管理对象

在Internet的第二版管理信息库MIB-II中，为SNMP应用实体定义了若干管理对象，其中包括SNMP的各种服务原语、各种收发协议数据单元、各种参数指示或统计变量等，凡SNMP中可操作的数据结构或变量都包括在内，下面将详细介绍。

2. MIB-II

在TCP/IP网络管理的建议标准中，提出了多个相互独立的MIB，其中包含为Internet的网络管理而开发的MIB-II。鉴于它在说明标准MIB的结构、作用和定义方法等方面的重要性和代表性，有必要对其进行比较深入的讨论。

MIB-II是在MIB-I的基础之上开发的，是MIB-I的一个超集。MIB-II组被分为以下分组：

- system 关于系统的总体信息。
- interface 系统到子网接口的信息。
- at(address translation) 描述Internet到子网的地址映射。
- ip 关于系统中IP的实现和运行信息。
- icmp 关于系统中ICMP的实现和运行信息。

- tcp　关于系统中 TCP 的实现和运行信息。
- udp　关于系统中 UDP 的实现和运行信息。
- egp　关于系统中 EGP 的实现和运行信息。
- dot3(transmission)　有关每个系统接口的传输模式和访问协议的信息。
- snmp　关于系统中 SNMP 的实现和运行信息。

(1) system 组

system 组提供有关被管系统的总体信息。

(2) interfaces 组

interfaces 组包含实体物理接口的一般信息，包括配置信息和各接口中所发生的事件的统计信息。

(3) address translation 组

address translation 组由一个表构成，表中的每一行对应系统中的一个物理接口，提供网络地址向物理地址的映射。一般情况下，网络地址是指系统在该接口上的 IP 地址，而物理地址决定于实际采用的子网情况。例如，如果接口对应的是 LAN，则物理地址是接口的 MAC 地址；如果对应 X.25 分组交换网，则物理地址可能是一个 X.121 地址。

实际上，address translation 组包含在 MIB-II 中只是为了与 MIB-I 兼容，MIB-II 的地址转换信息在各个网络协议组中提供。

(4) ip 组

ip 组包含有关节点上 IP 实现和操作的信息，如有关 IP 层流量的一些计数器。ip 组中包含 3 个表，ipAddrTable、ipRouteTable 和 ipNetToMediaTable。

ipAddrTable 包含分配给该实体的 IP 地址的信息，每个地址被惟一地分配给一个物理地址。

ipRouteTable 包含用于互联网路由选择的信息，该路由表中信息是从一些协议的路由表中抽取而来的。实体当前所知的每条路由都有一个条目，表格由 ipRouteDest 索引。ipRouteTable 中的信息可用于配置的监测，并且由于表中的对象是 read-write 的，因此也可被用于路由控制。

ipNetToMediaTable 是一个提供 IP 地址和物理地址之间对应关系的地址转换表。除了增加一个指示映射类型的对象 ipNetToMediaType 之外，表中所包含的信息与 address translation 组相同。

此外，ip 组中还包含一些用于性能和故障监测的标量对象。

(5) icmp 组

ICMP(Internet Control Message Protocol)是 TCP/IP 协议族中的一部分，所有实现 IP 协议的系统都提供 ICMP。ICMP 提供从路由器或其他主机向主机传递消息的手段，它的基本作用是反馈通信环境中存在的问题。例如：数据报不能到达目的地，路由器没有缓冲区来转发数据报。

icmp 组包含有关一个节点的 ICMP 的实现和操作的信息，具体地讲，icmp 组为节点接收和发送的各种 ICMP 消息的计数器所构成的一个表。

(6) tcp 组

tcp 组包含有关一个节点的 TCP 的实现和操作的信息。

(7) udp 组

udp 组包含有关一个节点的 UDP 的实现和操作的信息。除了有关发送和接收的数据报的信息之外，这个组中还包含一个 udpTable 表，该表中包含 UDP 端点的管理信息。所谓 UDP 端点是指正在支持本地应用接收数据报的 UDP 进程。udpTable 表中包含每个 UDP 端点用户的 IP 地址和 UDP 端口。

(8) egp 组

egp 组包含有关一个节点的 EGP(External Gateway Protocol)的实现和操作的信息。除了有关发送和接收的 EGP 消息的信息外，这个组中还包含一个 egpNeighTable 表，该表中包含有关相邻网关的信息。

3. RMON

简单网络管理协议 SNMP 是基于 TCP/IP 并在 Internet 中应用最广泛的网管协议，但是 SNMP 也有一些明显的不足，主要有以下 4 点：

- 由于 SNMP 使用轮询采集数据，而在大型网络中轮询会产生数量巨大的网络管理通信报文，导致网络交通拥挤甚至阻塞，故不适合管理大型网络。
- 不适合回收大信息量的数据，如一个完整的路由表。
- 基于 SNMP 的标准仅提供一般的验证，不能提供可靠的安全保证。
- 不支持 Manager-to-Manager 的分布式管理，它将收集数据的负担加在网管站上，使其成为瓶颈。

为了提高传送管理信息的可用性，减少管理站的负担，满足网络管理员监控网段性能的需求，IETF 开发了 RMON 以解决 SNMP 在日益扩大的分布式互联中的局限性。

远程网络监视(RMON)首先实现了对异构环境进行一致的远程管理，它为通过端口远程监视网段提供了解决方案。RMON 是 IETF 定义的 MIB(RFC1757)，是对 SNMP 标准的扩展，它定义了标准功能以及在基于 SNMP 管理站和远程监控者之间的接口，主要实现对一个网段乃至整个网络的通信流量的监视功能，目前已成为网络管理标准之一。它可以对数据网进行防范管理，使 SNMP 更有效、更积极主动地监测远程设备，使网络管理员可以更快地跟踪网络、网段或设备出现的故障，然后采取防范措施，防止网络资源的失效。RMON MIB 的实现可以记录网络事件，即使在网络管理站没有与监控设备主动进行连接(脱机)的情况下也如此。另外，RMON MIB 也用于记录网络性能数据和故障历史，可以在任何时候访问故障历史数据以进行有效的故障诊断。使用这种方法减少了管理者同代理间的通信流量，使简单而有力地管理大型互联网络成为可能。

RMON 监视器可用两种方法收集数据：一种方法是通过专用的 RMON 探测仪，网管站直接从探测仪获取管理信息并控制网络资源，这种方法可以获取 RMON MIB 的全部信息；另一种方法是将 RMON 代理直接植入网络设备(路由器、交换机、Hub 等)，使其成为带 RMON Probe 功能的网络设施，网管站用 SNMP 的基本命令与其交换数据信息，收集网络管理信息，但这种方式受设备资源限制，一般不能获取 RMON MIB 的所有数据，大多数只收集 4 个组的信息。

RMON MIB 对网段数据的采集和控制通过控制表和数据表完成。RMON MIB 按功能分成 9 个组。每个组有自己的控制表和数据表(有些组二者合一，如统计组)。其中，控制表可以读写，数据表只能读，控制表用于描述数据表所存放数据的格式。配置的时候，由

管理站设置数据收集的要求，存入控制表。开始工作后，RMON 监视器根据控制表的配置，把收集到的数据存放到数据表。

RMON MIB 包含以下 9 组数据：

(1) 统计组(Statistics)

统计组统计被监控的每个子网的基本统计信息。网络管理员可以从 RMON 探针监测的设备端口获取一个网段的各种统计信息。目前只能对网络设备的以太网接口进行监控、统计，将来会扩展到包括更多接口的特定表格(如 FDDI)。它能统计一个网段的流量(如交通流量的总包数和总字节数)，统计各种类型包的分布(如广播包、多点广播包、不同大小包的数量)，还能统计各种类型错误包数、碰撞次数等。

(2) 历史组(History)

历史组定期地收集统计网络值的记录并为日后的处理把统计存储起来。它包含历史控制组和以太历史组两个小组。其中历史控制组主要用来设置采样间隔时间等控制信息；以太网历史组为网络管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

(3) 警报组(Alarm)

警报组允许网络管理站为网络性能(可以是监视器本地 MIB 的任意整数类型的对象)定义一组报警阈值。如果阈值在相应的方向上被越过，监视器就会产生警报并把警报发往网络管理站。警报组需要事件组的实现。

(4) 主机组(Host)

主机组包含对连接在一个子网上所有主机的各种类型交通流量的记数值。它能够发现网上的新主机，对每个主机的 MAC 地址保持一组统计数据，例如，主机发送或接收的数据包总数、广播包数、流量字节数、错误包数等。它有一个控制表和两个数据表，其中，这两个数据表的内容相同，只是组织排列顺序不同。

(5) 最高主机组(Host Top)

最高主机组包括排序后的主机统计，该报告基于主机表中一些参数生成列表。它用于统计在一个子网上一些参数最高的一组主机，例如，它可以列出 10 个传输数据最多的主机，但依赖于主机组的实现。

(6) 矩阵组(Matrix)

矩阵组用于记录关于子网上两个主机之间流量的信息，该信息以矩阵形式存储起来。这种方法对于检索特定主机之间的流量信息十分有用，例如，用于找出哪些设备对服务器的使用最多。矩阵组由三个表组成，一个控制表加上两个数据表。

(7) 过滤组(Filter)

过滤组允许监视器观测与过滤器相匹配的数据包。网络监视器可以捕获所有通过过滤器的数据包或简单地记下基于这些数据包的统计。

(8) 包捕获组(Capture)

包捕获组控制数据被发往网管站的方式，它可以在把报文发送到某个通道后记录数据报文。

(9) 事件组(Event)

事件组提供关于 RMON 代理所产生的所有事件的列表。当某事件发生时可以记录日志

和发送 IRAP 到网管站。

尽管 RMON 有很多优点，但也有其局限性。RMON 的 MAC 层探测器不能确定由服务器进入本地网段的数据包的源点和终点，或者是不能确定经过被监视网段的通信数据包的源点和终点。

1994 年，RMON2 工作组开始致力于提高现存的物理层和数据链路层之间的 RMON 规范，以实现在网络和应用层提供历史和数据统计服务。图 5.4 说明了 OSI 参考模型与 RMON 相关的规范。

在网络层，RMON2 通过监视点对点通信来记录网络使用的模式。另外，RMON2 还显示单个应用所占用的带宽，以及出现疑难故障的关键因素。

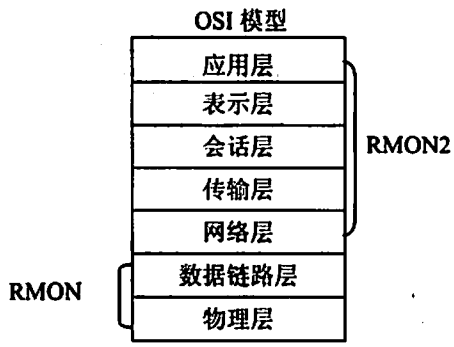


图 5.4 RMON 和 RMON2 所支持的协议层

5.1.1.4 利用工具监视网络性能

网络性能信息收集方案包括以下几点：

- Internet 控制消息协议 ICMP Ping
- 网络分析仪或探测器
- NetFlow

1. ICMP Ping

ping 对网络专业人员来说是一个常用且对用户友好的故障排除技术。ping 是一个工具，它使用 ICMP 返回请求和响应协议来测试与 IP 地址的连接性，能够快速浏览从工作站到目标 IP 地址的设备可达性和响应时间。然而，从工作站到远程节点使用 ping 可能无法确定问题的位置，因为测量可能发生在不同网络路径或多跳上。此外，使用 ICMP 测量响应时间不能准确反映应用的响应时间。一个透明、正常的网络(例如，具有快速 ping 响应和低使用率的网络)可能仍然掩盖着潜在的响应时间问题，因为问题可能处在协议栈的上层中。

2. 网络分析仪或探测仪

网络分析仪或探测仪是监测和解决响应时间问题的常用工具。探测仪通常是一个用于监测网络段性能的专用硬件设备。例如，RMON2 探测仪可以分析现有网络业务并报告所连网络段的使用率、顶层会话者和会话；这些报告都被上层协议分开。探测仪可捕捉分组并分析分组的头信息，用于深入分析网络段的活动。

探测仪关于网络段利用率和错误数的报告可以帮助网络专业人员准确确定网络时延和问题。然而，需要在应用路径的每一跳上设置许多探测仪以检测网络时延所处的位置。尽管网络分析仪或探测仪可以得到有价值的信息，但在解决响应时间和可用性问题上可能不是合算的方案。当校准网络或分析链路、协议和应用使用率趋势以及描述和识别最高层上对话者和会话时，专用探测仪更合适。

3. NetFlow

Cisco IOS NetFlow 技术收集并测量进入特定路由器或交换机接口的数据，是 Cisco IOS 软件的一个组成部分。

通过分析 NetFlow 数据，网络管理人员能够确定拥塞原因、每个用户的 CoS 以及应用，并确定业务的源网络和目的网络。NetFlow 支持极高的粒度和准确的业务测量以及高级聚合业务收集。由于它是 Cisco IOS 软件的一个组件，因此 NetFlow 支持基于 Cisco 产品的网络以实现 IP 业务流分析，而无需购买客户探测仪，从而使大型 IP 网络上的业务分析更经济。

5.1.1.5　利用工具监视网络故障

网络监视工具种类较多，此处仅介绍 OpenView、NetView、SunNet Manager 和其他一些常用的监视工具。

1. HP 的 OpenView

HP 的 OpenView 是第一个真正兼容的、跨平台的网络管理系统，因此也得到了广泛的市场应用。虽然 OpenView 被认为是一个企业级的网络管理系统，但它跟大多数别的网络管理系统一样，不能提供 NetWare、SNA、DECnet、X.25、无线通信交换机以及其他非 SNMP 设备的管理功能。

OpenView 不能处理因为某一网络对象故障而导致的其他对象的故障。

另外，在 OpenView 中，性能的轮询与状态的轮询是截然分开的，这样将导致一个网络对象响应性能轮询失败，但不触发一个报警，仅仅只有当该对象不响应状态的轮询才进行故障报警，这将导致故障响应时间的延长。

OpenView 还使用了商业化的关系数据库，这使得利用 OpenView 采集到的数据开发扩展应用变得相对容易。

2. IBM 的 NetView

NetView 既可以作为一个跨平台的、即插即用的系统提供给最终用户，也可以作为一个开发平台，在上面开发新的网络管理应用。它也不能提供 NetWare、SNA、DECnet、X.25、无线通信交换机以及其他非 SNMP 设备的管理功能。NetView 产品系列包括一个故障卡片系统，一些新的故障诊断工具，以及一些 OpenView 所不具备的其他特性。

NetView 不能对故障事件进行归并，不能找出相关故障卡片的内在关系，因此对一个失效设备，即使是一个重要的路由器，也将导致大量的故障卡片和一系列类似的警报。因此，NetView 不具备在掌握整个网络结构情况下管理分散对象的能力。在一个大型、异构网络中，这意味着服务的开销不能轻易地从网络开销中区分出来。

同样的，在 NetView 中，性能轮询与状态轮询也是彻底分开的，这也将导致故障响应

的延迟。NetView 也使用了商业化的关系数据库，这使得利用 NetView 采集来的数据开发扩展应用变得相对容易。

3. Sun 的 SunNet Manager

SunNet Manager(SNM)是第一个重要的基于 Unix 的网络管理系统。SNM 一直作为主要开发平台而存在，但它仅提供了很有限的应用功能。为了实用化，还必须附加很多第三方开发的针对具体硬件平台的网络管理应用。SNM 跟其他大多数网络管理系统一样，也不能提供 NetWare、SNA、DECnet、X.25、无线通信交换机以及其他非 SNMP 设备的管理功能。

SNM 有两个特性：Proxy 管理代理和集成控制核心。

4. 其他常用工具

网络故障检测还经常用到一些命令，如 ping，traceroute，nslookup，netstat，arp 以及 route 等。

(1) ping

ping 命令是网络中使用最频繁的测试命令，它的协议基础是 TCP/IP 中的 ICMP。

ping 命令发出 ICMP 的 Echo 消息，接收者听到后应答 ICMP 的 Echo 应答消息，这一问一答就表明源站与目的站间的 TCP/IP 协议正常地运行连通。ping 命令还具有测试网络响应时间的功能，以问答间隔为标准。在配置管理功能中的网络拓扑图的自动发现就用 ICMP 协议以类似于 ping 命令的方式完成。

(2) traceroute

traceroute 命令是用来测试 IP 数据包到达目的端经过的所有路由器的路径及连通状况，它显示每一个路由器的响应时间来反应速度快慢，在测试路由协议的配置时经常使用。

(3) netstat

netstat 命令是显示 TCP/IP 协议状态的命令，工作站中的网络问题由此命令进行分析。

(4) nslookup

nslookup 命令用于向 DNS 服务器发送一个 DNS 查询，对完整的域名和 TCP/IP 地址进行查询解析，然后显示 DNS 服务器名称、地址和解析到的信息。

(5) Cisco Management Station to Device

如果一个设备可以对 ping 或者 traceroute 进行响应，但是却不能支持 SNMP 或者其他第 4 层的应用，则可以使用这个工具来测试应用方面的问题。这个工具可以用来测试 UDP，TCP，HTTP，TFTP，Telnet 和 SNMP 的连接是否正常。对于 UDP 和 TCP，所测试的端口为 7，对于其他的协议，将测试服务器一侧的端口。对于各个应用来说，这个工具就像是一个客户端。为了取得测试成功，在设备上必须运行以上提及的协议，将之作为一个 Server。例如，为了取得 HTTP 测试的成功，需要使用 ip http server 命令在路由器上启动 Web 接口。如果使用的是主机名而不是 TCP/IP 地址，则在测试之前将首先对主机名进行解析并将解析的结果显示出来。

(6) Network Show Command 应用

Network Show Command 应用是一个基于 Java 的工具，通过这个工具，管理员可以定义用户针对其 Cisco 设备运行的 show 命令列表。Network Show Command 还提供了一个可选的远程控制台选项，在这个控制台上，可以输入 show 命令列表中没有定义的 show 命令。

Network Show Command 工具存在的问题是它的权限控制操作十分复杂，权限严格限制了用户可以执行的命令，但是并不限制它能够完成的功能。当把 Network Show Command 工具和 NetConfig 工具一起使用的时候，用户只有有限的特权，只能配置网络设备上的某些属性，根据 NetConfig 应用中的模板来修改设备的配置，这些模板是由管理员创建的。用户通过 Network Show Command 工具，可以验证 NetConfig 任务的输出结果。另外一个优点是 Network Show Command 工具和 NetConfig 工具可以一次性对多个设备产生影响，比较高效。

5.1.1.6　利用工具监视网络安全

1. 入侵检测系统

入侵检测系统是近几年出现的新型网络安全技术，它试图发现入侵者或识别出对计算机的非法访问行为，并对其进行隔离。入侵检测系统能发现其他安全措施无法发现的攻击行为，并能收集可以用来诉讼的犯罪证据。

入侵检测系统有两类：基于网络的实时入侵检测系统和基于主机的实时入侵检测系统。目前 IDS 解决方案和产品有很多种，这里介绍的入侵检测产品包括 ISS 公司的 RealSecure、Cisco 的 IDS 和清华紫光 UnisIDS。

2. 入侵检测产品介绍

(1) RealSecure

RealSecure 是一个计算机网络上自动实时的入侵检测和响应系统，也是全球惟一一个被权威机构评测为 B+级的实时监控网络安全入侵软件。RealSecure 提供实时的网络监视，并允许用户在系统受到危害之前截取和响应安全漏洞和内部网络误用。RealSecure 无妨碍地监控网络传输并自动检测和响应可疑的行为，从而最大程度地保障企业信息安全。

RealSecure 的优点有：

- 对网络攻击实时响应。
- 记录攻击事件以便于回放。
- 最广泛的攻击模式识别。
- 内置的报告生成。
- 很大范围的网络拓扑。
- 事件响应的在线帮助数据库。
- 运行在包括 Windows NT 和 Unix 平台等多种平台之上。
- 监控 Windows 的网络和 TCP/IP 传输。
- 对网络传输流无影响。

在每台需要保护的主机上安装 RealSecure 的主机监控模块，System RealSecure 可以实时监视各种对主机的访问请求，并及时将信息反馈给控制台。这样，全网任何一台主机受到攻击时，系统都可以及时发现，并可将反馈信息及时传送给控制台进行处理，并能自动对入侵事件做出反应。

在需要重点保护的网段，也要安装 RealSecure 的网络监控模块，对这一网段的非正常的访问进行监视。考虑到管理的方便性和可行性，最好在网络上设置一台网管工作站作为网络检测的控制台。

(2) Cisco IDS 解决方案

考虑到企业站点非常复杂，攻击技术多种多样，黑客数量只增不减，必须采用全面的解决方案才能有效预防黑客袭击。这种解决方案应该能对抗多种攻击技术，并防止在典型攻击过程中执行的恶意操作。由于 Cisco IDS 解决方案提供包含 NIDS 和 HIDS 组件的组合解决方案，因而能满足这个要求。NIDS 主要预防网络袭击，HIDS 则主要防止服务器的 OS 操作系统和应用遭受袭击。

NIDS 检测器安装在多个位置上，最重要的位置是防火墙前面，负责监控进入机构的通信信息。另外，每个重要的网段都安装一个检测器。HIDS 首先部署在面对互联网的服务器上，例如 Web、邮件和 DNS 服务器。由于面向互联网的服务器与后端服务器相连，因此，HIDS 也部署在公司防火墙内的所有其他主要服务器上。

① Cisco IDS 网络检测器

网络检测器能够为网络设备及服务器上的通信模块提供全面保护。其主要特性包括：

- 积极响应(系统包含对检测器设备的主动响应功能)。
- 全面检测网络袭击。
- 全面检测应用袭击。
- 以独特的方式预防 DoS(Deny of Services，拒绝服务攻击)。
- 先进的 IP 分片重装和 Whisker 反 IDS 检测功能支持。

② Cisco IDS 主机检测器

主机检测器能够为服务器上运行的服务器操作系统和应用提供全面保护。主机检测器安装在每台服务器上，用于保护操作系统和应用。系统利用呼叫截获技术提供纯主动式服务器安全系统。其主要特性包括：

- 现场预防操作系统和应用袭击。
- 防止缓冲器溢出袭击。
- 不断提高完整性。
- Web 服务器屏蔽。
- 防止安全套接层(SSL)加密的 HTTP 袭击。

(3) 清华紫光 UnisIDS

清华紫光公司的 UnisIDS 是一套面向访问数据量庞大的局域网用户的网络入侵监测系统，这套软件包括管理中心 Admin 和基于网络的入侵检测引擎 Network Agent(清华紫光还推出了基于主机的入侵检测引擎 Host Agent)。该系统庞大的网络入侵知识库包含了大多数网络攻击的特征，能提前、主动地检测到来自网络的各种恶意攻击。

Network Agent 安装在局域网中作为网络连接节点的计算机上，它能通过对网络数据包的实时分析，检测和发现各种不同类型的网络攻击(如 IP 地址扫描、“拒绝服务”式攻击等)和入侵者难以消除的入侵痕迹；还能完成检测、防止错误网络操作、分析和监控网络流量、防止机密资料的流失、记录事件日志等任务。一旦发现可疑的入侵行为和异常数据包，Network Agent 会通知管理员人工采取应对措施，或自主截断入侵。

Admin 是 UnisIDS 的管理中心，可以安装在局域网上的任何一台计算机上，能通过对配置和策略的管理集中控制引擎的工作，对网络和服务器的状态进行实时监视，并可以生成各种统计报表。

UnisIDS 入侵检测系统能为通过因特网进行的电子商务环境提供最完整的安全解决方案，采用方便且全面的方法对入侵进行检测、截断、报警并提供入侵日志。UnisIDS 入侵检测系统的用户对象是网络安全管理者、信息安全咨询公司、信息安全法律执行机关、大中型企业、因特网服务及内容提供商、教育以及政府机构。

3. 漏洞扫描安全评估技术

(1) 概述

漏洞扫描安全评估技术可以帮助网络管理者对网络的安全现状进行扫描，并在发现漏洞后提出具体的解决办法。

网络安全漏洞扫描系统通常安装在一台与网络有连接的主机上。系统中配有一个信息库，其内存放着大量有关系统安全漏洞和黑客攻击行为的数据。扫描系统根据这些信息向网络上的主机和网络设备发送数据包，观察被扫描的设备是否存在与信息库中记录的内容相匹配的安全漏洞。扫描的内容包括主机操作系统本身、操作系统的配置、防火墙配置、网络设备配置以及应用系统等。

通过网络扫描，系统管理者可以及时发现网络中存在的安全隐患，并进行必要的修补，从而减小网络被攻击的可能。

(2) 安全扫描方式

安全扫描方式包括直接配置检查和模拟入侵两种。

① 直接配置检查　这种技术的代表是 COPS(Computer Oracle Password and Security system)。COPS 从系统内部常见的 Unix 安全配置错误与漏洞(如关键文件权限设置、ftp 权限与路径设置、root 路径设置、密码等)入手，指出系统内存在的安全问题，从而减少系统可能被入侵者(包括内部用户)利用的漏洞。

② 模拟入侵　这种技术模拟入侵者可能的攻击行为，从系统外部进行扫描，以探测是否存在可以被入侵者利用的系统安全薄弱之处。其代表有 ISS(Internet Security Scanner)和 SATAN(Security Analysis Tool for Auditing Network)。

(3) 安全扫描工具

安全扫描工具通常也分为基于服务器和基于网络的扫描器。

基于服务器的扫描器主要扫描服务器相关的安全漏洞，如 password 文件、目录和文件权限、共享文件系统、敏感服务、软件、系统漏洞等，并给出相应的解决办法建议。通常与相应的服务器操作系统紧密相关。

基于网络的安全扫描主要扫描设定网络内的服务器、路由器、网桥、交换机、访问服务器、防火墙等设备的安全漏洞，并可设定模拟攻击，以测试系统的防御能力。通常该类扫描器限制使用范围(IP 地址或路由器跳数)。

5.1.1.7　性能监视的检查点

网络性能包括带宽利用率、吞吐率降低的程度、通信繁忙的程度、网络瓶颈及响应时间等，这些参数的控制和优化是系统管理人员的日常性工作。性能指标通过性能监测设备采集并存储在数据库中。数据库可以放在代理中，也可以放在管理站中，这取决于代理和管理站的能力以及通信开销的大小。

如果数据量太大，可以只存储统计摘要和趋势分析的结果。在 ISO 10165-2(管理信息

定义)中定义的管理对象的某些属性代表了系统的性能参数。这些属性是：

- 计数器(Counter) 计数器的特点是初始值为零，其值只能增加不能减少，增加到最大值时归零。它的应用很广泛，例如：可以用来表示工作站接收的分组数。
- 计量器(Gauge) 与计数器不同，计量器的值可增加也可减少，达到最大值时不归零，而是不再增加，但可以减少。例如：可以用它表示网络层实体管理的队列长度。
- 阈值(Threshold) 阈值可用于计数器或计量器。当计数器的值达到某个阈值时管理对象要发出通知。计量器的阈值有两个，分别是上限和下限，并且仅当被监视的量的变化经过上/下限时，管理对象才发出报警通知。
- 涨潮点(Tidemark) 指计量器的最低点或最高点。涨潮点属性有 3 个值即当前值、最近一次复位之前的值和最近复位的时间等。后两个值可用来计算潮汐的大小和到达涨潮点的时间。

5.1.1.8 系统性能分析

性能分析功能要完成以下任务：

- 对监测到的性能数据进行统计和计算，获得网络及其主要元素的性能指标，定期产生性能报表。
- 负责维护性能 MIB，存储网络及其主要元素性能的历史数据。
- 根据当前数据和历史数据对网络及其主要元素的性能进行分析，获得性能的变化趋势，分析制约网络性能的瓶颈问题。
- 在网络性能异常的情况下向网络管理者进行告警，在特殊情况下，直接启动故障管理功能进行反应。

性能分析的基础是建立和维护一个有效的性能 MIB。在此基础上，要解决的关键问题是设计和构造有效的性能分析方法。传统的方法是基于解析的方法。

解析的方法又分为预测法和解释法两种。预测法是根据网络的结构以及各个网络元素的性能，推测网络的总体性能的方法。解释法是从网络的结构以及观测到的总体性能出发，推测各个网络元素性能的方法。基于解析的方法具有局限性，因此对于比较复杂的关系难以迅速得到正确结果。

现在，基于人工智能的网络性能分析方法越来越受到重视。在这种方法中，一般利用专家系统对网络性能进行分析，提高了分析的水平和速度。

5.1.1.9 安全监视的检查点

安全管理的目的是提供信息的保密、认证和完整性保护机制，使网络中的服务、数据以及系统免受侵扰和破坏。目前采用的网络安全措施主要包括通信伙伴认证、访问控制、数据保密和数据完整性保护等。一般的安全管理系统包含风险分析功能，安全服务功能，报警、日志和报告功能，网络管理系统保护功能等。

需要明确的是，安全管理系统并不能杜绝所有的对网络的侵扰和破坏，其作用仅在于最大限度地防范，以及在受到侵扰和破坏后将损失尽量降低。具体地说，安全管理系统的主要作用有以下几点：

- 采用多层防卫手段，将受到侵扰和破坏的概率降到最低。
- 提供迅速检测非法使用和非法入口的手段，核查跟踪侵入者的活动。
- 提供恢复被破坏的数据和系统的手段，尽量降低损失。
- 提供查获侵入者的手段。

5.1.2　典型例题分析

例 1　下面哪个类型的设备可以收集网络的信息，例如：包的尺寸、包的数量、包的错误、连接的利用率和通信的负载？

- 模型和仿真工具
- 协议分析器
- 网络监视器
- 网络管理系统
- TDR

分析：网络监视器用来收集网络信息，例如包的尺寸、数量、错误，连接的利用率以及通信和负载。

协议分析器用来捕获、显示和分析给定网络中的多层协议。

网络管理系统通常可以进行网络的故障、账户、性能的管理和通过 SNMP 的远程设备进行的安全管理。

TDR 和 OTDR 用来检测铜缆和光纤故障，如开路、短路、弯曲、结头或不当阻抗匹配。

答案：网络监视器。

例 2　下面哪一个命令可以在一个交换机上查看关于与系统 LED 相应的指示灯的状态、交换机运行时间、当前通信的负载、通信负载的峰值和其他系统相关的信息？

- show system
- show version
- show startup-config
- show nvram
- show flash

分析：show system 命令用来显示标识状态与系统 LED 相应的指示灯的状态、交换机运行时间、当前通信的负载、通信负载的峰值和其他系统相关的信息。例如：

```
Catalyst(enable) show system
ps1-status  ps2-status  Fan-status  temp-alarm  uptime  d,h:m:s logout
----------  ----------  ----------  ----------  -------  ------  ------
ok          ok          ok          off         259     09:09:23 10min
```

答案：show system

例 3　假定需要为一个桥接器厂商编写符合 SNMP 的代码，你读了所有的 RFC 但仍然有问题。你向 IAB 建议在某个地方给出用来描述 SNMP 变量的语言一个完整的形式语法，

IAB 的反应是同意并指定你做这一工作。这个语法应被加入 RFC1442 或 RFC1213 吗？为什么？

分析：SMI(管理信息结构，RFC1442)给出了定义数据类型的规则。MIB(管理信息库，RFC1213)是使用这些规则产生的实例定义。因此 SMI 像是程序设计语言描述，而 MIB 则像是以该程序设计语言编写的程序(实际上更像是 C 语言的程序头，而不是真正的程序)。所以所给出的形式语法应被加入 RFC1442，因为该 RFC 已经描述了 ASN.1 的限制条件，但尚无所允许子集的形式语法。

答案：所给出的形式语法应被加入 RFC1442，因为该 RFC 已经描述了 ASN.1 的限制条件，但尚无所允许子集的形式语法。

例 4 什么是 RMON 组？

答案：RMON MIB 按功能分为 9 个组，包括：统计组、历史组、警报组、主机组、最高主机组、矩阵组、过滤组、包捕获组和事件组。

例 5 什么是网络管理代理？

答案：网络管理代理是被管设备(被管理的对象)上收集和存储管理信息的软件。

例 6 RMON 如何简化前摄性网络管理？

答案：没有 RMON，MIB 用于检查各机器的网络性能将导致需要大量带宽来管理业务。通过使用 RMON，被管设备本身收集并存储数据(通过其 RMON 代理)，否则 MIB 必须频繁地检索它们。

5.1.3 同步练习

1. SNMP 管理员如何请求一个数据列表？
2. 什么是系统日志严重级别？
3. NetFlow 为什么优于 RMON?
4. 配置管理对网络管理员来说有何好处？配置管理使用哪些协议？
5. 网络中高延迟意味着什么？

5.1.4 同步练习参考答案

1. 首先管理人员发送一个 get-request 向代理请求特定的 MIB 变量。然后使用 get-nextrequest 消息从表中或列表中检索下一个对象实例。

2. 系统日志定义了下列严重级别：

紧急情况(第 0 级，它是最高级)；报警(第 1 级)；危急(第 2 级)；错误(第 3 级)；

警告(第 4 级)；注意(第 5 级)；信息性(第 6 级)；调试(第 7 级)。

3. NetFlow 信息收集的益处包括：有关收集数据、数据时间戳的更详细的信息，对每个接口不同数据的支持以及更好的可扩展性。NetFlow 的性能影响相比 RMON 要更低，而且无需外部探测器。NetFlow 服务利用网络业务的流特性以对路由器性能最小的影响来

收集详细的数据，以便高效地处理用于分组过滤和安全性服务的数据列表。

4. 配置管理的好处包括以下几点：
- 由于反应性问题减少，因此支持费用更低。
- 识别未用网络组件的设备、电路和用户跟踪工具以及程序降低了网络费用。
- 由于反应性支持费用的减少，从而改善了网络的可用性以及缩短了问题解决的时间。
- 配置管理使用的协议：SNMP、TFTP 以及 Telnet。

5. 高延迟值可能表示端设备或者路由器、交换机等中继设备上存在拥塞。

5.2 故障恢复分析

5.2.1 考点辅导

5.2.1.1 故障分析要点

故障定位是在一个给定的系统中检测、隔离和修理故障的过程。

一个网络是一个动态系统，对于一个动态的系统而言，故障定位的主要挑战在于，如何在许许多多的部件中隔离出故障部件来。有经验的故障定位人员和网络技术人员遵循一套精心设计的过程来诊断一个问题的来源。

进行故障定位所遵循的规则实际上是在基于一些常识的基础上进行的，例如：
- 确定问题的实际性质
- 隔离问题的原因
- 解决问题

“确定—隔离—解决”这 3 个步骤在大部分网络中都能够成功地奠定对问题故障定位的基础，如图 5.5 所示。

1. 识别故障现象

知道出了问题并能够避免，是进行成功故障定位的最重要的步骤。大部分网络问题是通过某些现象表现出来的。所以在遇到问题时，要想高效地解决问题，首先必须能对问题进行定位，这就需要设法收集到一些与问题可能有关的线索。需要强调的一点是在确定问题的实际性质之前，必须知道系统的正常运行特性(即基线)。

2. 对故障现象进行详细描述

如果得到一个差错消息，应将屏幕显示的内容记录下来，并将该差错信息写在一个网络差错日志中。差错消息的内容以及差错显示的位置(是显示在服务器上还是显示在客户机上)信息，对于判断该差错发生的位置是一个重要的线索。

所以，一定要在网络配置日志中对每个硬件和软件的改变做详细的记录。一旦对能够观察到的一切现象都收集到了，就可以依赖经验形成一个假设。

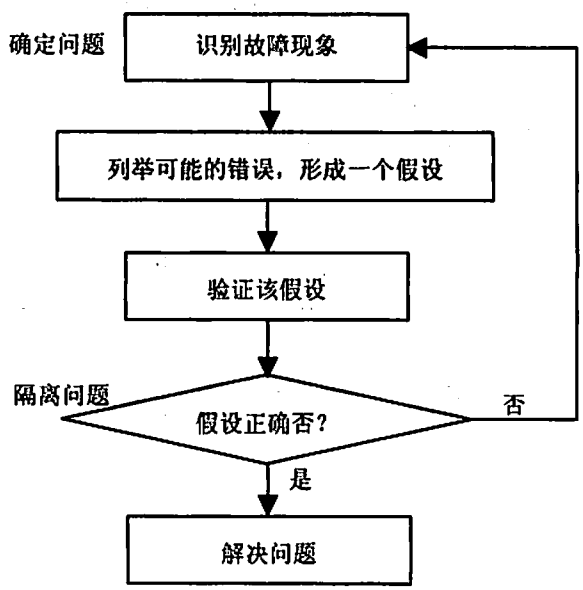


图 5.5 诊断网络问题的循环过程

3. 列举可能的错误并形成假设

列举出所有可能导致被监测到的故障现象，然后，利用有效的工具剔除各种可能的误报故障，根据最终结果形成一个关于故障的假设。

在故障定位中，经验和专门知识是非常有用的。为了使假设与这些现象相一致，必须熟悉网络问题的类型，才能从正常出现的网络问题中分辨出这些故障现象，同时也需要深入理解运行在该网络上的相关协议和应用程序。

4. 隔离问题的来源

确定问题可能的来源后，则应该针对不同原因分别进行测试。当决定这样做时，应当能够确定假设的正确性。

5. 验证假设

可以使用几种方法来验证假设的正确性。专家们经常使用的一种方法是“替换法”，即用确知可以正常工作的类似部件来替代怀疑存在问题的部件。在熟悉每个部件的性能以及它们可能引起的后果时，使用这个方法比较有效。

6. 得出结论

针对每个假设进行的实验，必须确定该假设是否正确。如果该问题依然存在，则可判断该假设是不正确的。如果该问题已经解决了，则表明已经找到了该问题的根源。其中最为麻烦的一种情况是，当替换掉部件之后，问题依然存在，但外在表现形式却不同。随着积累的经验越来越多，将逐渐知道对于每个可能的实验的结果，其结论会是什么。对于一个具有可能不熟悉的测试结果的实验，应该扩展或修订关于该问题的方法，从而能够更好地将所观察到的测试结果与收集到的现象联系在一起。

故障的定位过程是一个循环的过程。如果一个测试的结果没有得出结论，必须重新详细地分析该问题所表现出的现象，从而形成新的假设。在大多数情况下，需要在重新检查

该现象之前，变换一下该问题的环境。

7. 解决问题

一旦完成隔离出所有故障的部件后，必须对此故障进行修复。围绕有问题的部件进行修理、更换或处理。对于有故障的硬件，惟一的选择就是修理或更换该部件。对于软件，通常可以通过重新安装或删除来修复该问题。

5.2.1.2　局域网监控程序

一旦发现了用户错误或物理连接问题(包括网线损坏)，一些网络监控工具(包括网络监视器和分析仪)会帮助分析网络流量、捕捉和分析网络上的数据，进行一个更深入的分析。

1. 网络监视器和分析仪

一个网络监视器是基于软件的工具，它可以在连到网络上的一台服务器或工作站上持续监测网络流量，网络监视器一般工作在 OSI 模型的第三层，可以检测出每个包使用的协议，但是不能破译包里的数据。

一个网络分析仪是便携的、基于硬件的工具。网络管理员把它连入网络，专门用来解决网络问题，网络分析仪可以破译直到 OSI 模型第七层的数据，例如，分析仪可以辨别一个使用 TCP/IP 的包，甚至可以辨别它是从特定工作站到服务器的 ARP 应答信号。分析仪可以破译包的负载率，把它从二进制码转换为易读的十进制或十六进制码，因此，网络分析仪可以捕获运行于网络上的密码(只要它们的传输不是加密的)，一些网络测试仪软件包可以在标准 PC 机上运行，但有的需要在带特殊网络接口卡和操作系统软件的 PC 机上运行。

网络监视工具通常比网络分析仪便宜，并且可能包含在网络操作系统软件中，下面介绍其中的两种：Microsoft 的 Network Monitor(附于 Windows NT Server Version 4.0 及以后系统)和 Novell 的 LANalyzer agent(附于 Novell's manage wise software package)，其他的产品有类似的工作方式，大多数甚至使用非常相似的图形界面。

注意：为了利用基于软件的网络监视器和分析仪，计算机上的网络接口卡必须支持随机模式，随机模式是指设备驱动程序引导网络接口卡接收流过网络的所有帧，不光是指向该节点的帧。

(1) 微软的网络监视器

Network Monitor(NetMon)是基于软件的且随 Windows NT Server 4.0 或者 Microsoft's Systems Management Server(SMS)一起的网络监视软件。它提供以下功能：

- 从网络一段或几段中捕获传输数据。
- 捕获来/去特殊节点的帧。
- 通过发送指定数量和类型的数据来重现网络状态。
- 检测在网络上 NetMon 的其他运行副本(依赖于路由器的位置和配置)。
- 产生网络活动的参数。

NetMon 最有用的能力是捕获网络上传输的数据，NetMon 观察网络一段时间，捕获通过特定网络的数据(因为 NetMon 利用随机模式，它捕获所有的数据，不仅是来/去 NetMon 控制台的数据)。然后，可以在 NetMon 中找出错误的帧，按照每个节点产生坏数据的多少按从大到小排序，一般在队列最前边的工作站就是问题所在，它产生了比其他节点多得多的坏数据包在网络上传输。

(2) Novell 的网络分析仪

Novell 提供了一个和 Microsoft's Network Monitor 相似的网络监视工具——LANalyzer 代理，它可作为一个独立的程序工作于 Windows 工作站或作为 Manage Wise 的一部分在 Netware 服务器上装配网络管理工具，LANalyzer 具有如下功能：

- 能发现网段上几乎所有网络节点
- 连续监测网络流量
- 当流量达到预定的阈值时报警(例如利用率超过 70%)
- 捕获来(或去)所有(或选定)节点的流量

像 Network Monitor 一样，LANalyzer 能按节点捕获流量和辨别错误数据，按网段产生流量参数，另外，作为 Manage Wise 的套件，LANalyzer 能在特定的网段上发现所有的节点。它可以利用这些数据构造网络管理系统，这个网络管理系统不仅可以收集信息(例如，发现一个用户在某一特定的工作站上登录的次数，记录工作站通向服务器申请程序的类型)，而且可以提供实时的网络参数，当达到网络阈值时发送提示信息或警告声音。

2. 网络分析软件

除了利用随同网络操作系统的软件，还可以从专门从事网络管理的提供商那里购买网络分析软件，一个典型的例子是网络联盟的 NetXRay，这个网络分析软件提供数据捕获、分析、发现节点、流量转向、记录、报警和利用率预测。NetXRay 与 Network Monitor 和 LANalyzer 有相同的特征，同时又增加了一些附属物，它也可以为了重现网络故障而产生流量和同时监测多个网络段，其图形界面使这个产品使用方便，显示网络流量的可读性强，NetXRay 支持多协议和网络拓扑结构。

另外网络联盟还牵头开发了基于硬件的网络分析仪，叫做探测器(sniffer)，探测器通常是装配了特殊的网络接口卡和网络分析软件的便携式电脑。探测器基本的工作是分析网络问题。探测器提供了它所能捕获到的大量的各种类型和深度的信息，用这种类型的工具的危险是它可能收集了超过计算机所能处理的信息，为了避免这个问题，应该为收集到的数据设置过滤器。

如果一个网络是全部交换的(即每个节点连接到自己的交换端口)，网络分析仪只能捕获到广播的包和目的地址为正运行软件的节点的包，因为在交换环境下，只有这些数据包才能传输到目的地址。交换机的使用使网络监视更加困难，解决方案是重新配置交换机来重新选择路由，这样网络分析仪才能接收到所有的流量，显然，应该权衡一下重新配置引起的破坏性和潜在的好处(能够分析网络流量和排除故障)。

5.2.1.3 排除故障要点

网络故障排除应按照规定的步骤进行，这样可以节省时间和经费(譬如不必要的软件、硬件替换等)。

1. 网络排错的步骤

网络排错的步骤如下所述：

(1) 认清症状。

(2) 验证用户权限。例如，确保用户正确输入了他或她的口令。

(3) 限定问题的范围。它是全局性的吗？即网上的所有用户总是会碰到这个问题吗？

或者问题只发生在网络上某一地理区域，某一特定的工作组，某一特定的时间段？换句话说，这问题是属于地区性的，工作组性的还是时间相关的?

(4) 重现故障，并且要保证能够可靠地重新产生这个错误。

(5) 验证网络物理连接(例如网络连线、网络接口卡的插槽、供电电源)的完整性。从受到影响的节点开始，向主干网延伸。

(6) 验证网络的软连接问题(例如地址、协议绑定、软件安装等)。

(7) 考虑最近的网络变更和可能因此导致的网络问题。

(8) 实施解决方案。

(9) 检验解决方案。

根据自己的观察，可以从上面列表中的一步跳到另一步，减少所执行的检查步骤。

2. 故障查找注意事项

由于以太网采用通用总线拓扑结构以及物理层可扩展的潜在问题，所以某个特定物理层的问题会以不同的方式显示出来，而且由于采用的测试手段、位置和环境不同，显示出的现象还常常相互矛盾。

为了避免被假象误导，可以按照以下两个步骤查找故障：

(1) 沿网段多做几次测试。如果故障现象随测试点的不同还保持一样，就可以依照所测试出的故障现象去排除。如果故障现象在一些或所有的测试点都不相同，就要把查找故障的方向定在物理层(除非有特别提示)，例如，去查找坏的电缆、噪声环境、接地循环等故障。

(2) 要提高测试质量。在测试的同时要把测试仪器设置成至少可同时发送较低的流量。由于增加了网络流量，微小的和间歇性的物理层问题就会暴露出来。

3. 网络故障诊断和排除

网络中可能出现的故障多种多样，解决一个复杂的网络故障往往需要广泛的网络知识与丰富的工作经验。这也是为什么一个成熟的网络管理机构制定有一整套完备的故障管理日志记录机制，同时人们也率先把专家系统和人工智能技术引进到网络故障管理中来的原因。另一方面，由于网络故障的多样性和复杂性，网络故障分类方法也不尽相同。

可以根据网络故障的性质把故障分为物理故障与逻辑故障，也可以根据网络故障的对象把故障分为线路故障、路由器故障和主机故障。

(1) 按照故障性质分类

① 物理故障。物理故障是指设备或线路损坏、插头松动、线路受到严重电磁干扰等情况。比如说，网络中某条线路突然中断，这时网络管理人员从监控界面上发现该线路流量陡然下降或系统弹出报警界面，此时首先用 ping 检查线路在网络管理中心的端口是否连通，如果不连通，则检查端口插头是否松动，如果松动则插紧，再用 ping 检查，如果连通则故障解决。这时需把故障的特征及其解决步骤详细记录下来。也有可能是线路远离网络管理中心的那端插头松动，则需要通知对方进行解决。另一种常见的物理故障就是网络插头误接。这种情况经常是没有搞清网络插头规范或没有弄清网络拓扑规划的情况下导致的。另一种情况，比如两个路由器直接连接，这时应该让一台路由器的出口连接另一路由器的入口，而这台路由器的入口连接另一路由器的出口才行，这时制作的网线就应该满足这一

特性，否则也会导致网络误接。不过像这种网络连接故障显得很隐蔽，要诊断这种故障没有什么特别好的工具，只能依靠经验。

② 逻辑故障。逻辑故障中的一种常见情况是配置错误，就是指因为网络设备的配置原因而导致的网络异常或故障；配置错误可能是路由器端口参数设定有误，或路由器的路由配置错误以至于路由循环或找不到远程地址，或者是网络掩码设置错误等。比如，同样是网络中某条线路故障，发现该线没有流量，但又可以 ping 通线路两端的端口，这时很可能就是路由配置错误导致循环了。诊断该故障可以用 traceroute 工具，可以发现在 traceroute 的结果中某一段之后，两个 IP 地址循环出现。这时，一般就是线路远端把端口路由又指向了线路的近端，导致 IP 地址在该线路上来回反复传递。这时需要更改远端路由器端口配置，把路由设置为正确配置，就能恢复线路了。当然处理该故障的所有动作都要记录在日志中。

逻辑故障中另一类故障就是一些重要进程或端口关闭，以及系统的负载过高。比如，路由器的 SNMP 进程意外关闭或死掉，这时网络管理系统将不能从路由器中采集到任何数据，因此网络管理系统失去了对该路由器的控制。还有，就是线路中断，没有流量，这时用 ping 发现线路近端端口 ping 不通，检查发现该端口处于 down 的状态，就是说该端口已经给关闭了，因此导致了故障，这时只需重新启动该端口，就可以恢复线路的连通了。

(2) 按故障对象分类

网络故障根据故障的不同对象可将网络故障划分为线路故障、路由器故障和主机故障。

① 线路故障。线路故障最常见的情况就是线路不通，诊断这种故障可用 ping 检查线路远端的路由器端口是否还能响应，或检测该线路上的流量是否还存在。

一旦发现远端路由器端口不通，或该线路没有流量，则该线路可能出现了故障。这时有几种处理方法。

首先是 ping 线路两端路由器端口，检查两端的端口是否关闭了。如果其中一端端口没有响应则可能是路由器端口故障。如果是近端端口关闭，则可检查端口插头是否松动，路由器端口是否处于 down 的状态；如果是远端端口关闭，则要通知线路对方进行检查。进行这些故障处理之后，线路往往就通畅了。

如果线路仍然不通，一种可能就得通知线路的提供商检查线路本身的情况，看是否线路中间被切断等；另一种可能就是路由器配置出错，比如路由循环了。就是远端端口路由又指向了线路的近端，这样线路远端连接的网络用户就不通了，这种故障可以用 traceroute 来诊断。解决路由循环的方法就是重新配置路由器端口的静态路由或动态路由。

② 路由器故障。事实上，线路故障中很多情况都涉及到路由器，因此也可以把一些线路故障归结为路由器故障。但线路涉及到两端的路由器，因此在考虑线路故障时要涉及到多个路由器。而有些路由器故障仅仅涉及到它本身，这些故障比较典型的就是路由器 CPU 温度过高、CPU 利用率过高和路由器内存余量太小。其中最危险的是路由器 CPU 温度过高，因为这可能导致路由器烧毁。而路由器 CPU 利用率过高和路由器内存余量太小都将直接影响到网络服务的质量，比如路由器上丢包率就会随内存余量的下降而上升。

检测这种类型的故障，需要利用 MIB 变量浏览器工具，从路由器 MIB 变量中读出有关的数据，通常情况下网络管理系统有专门的管理进程不断地检测路由器的关键数据，并及时给出报警。而解决这种故障，只有对路由器进行升级、扩内存等，或者重新规划网络的拓扑结构。另一种路由器故障就是自身的配置错误，比如配置的协议类型不对，配置的

端口不对等。这种故障比较少见，但没有什么特别的发现方法，排除故障就与网络管理人员的经验有关了。

③　主机故障。主机故障常见的现象就是主机的配置不当。比如，主机配置的 IP 地址与其他主机冲突，或 IP 地址根本就不在子网范围内，这将导致该主机不能连通。还有一些服务的设置故障，比如邮件服务器设置不当导致不能收发 E-mail，或者 DNS 服务器设置不当将导致不能解析域名。主机故障的另一种可能是主机安全故障，比如主机没有控制其上的 finger，rpc，rlogin 等多余服务。而恶意攻击者可以通过这些多余进程的正常服务或错误(bug)攻击该主机，甚至得到该主机的超级用户权限等。

另外，还有一些其他的主机故障，比如共享本机硬盘不当等，将导致恶意攻击者非法利用该主机的资源。发现主机故障是一件困难的事情，特别是别人恶意的攻击。一般可以通过监视主机的流量、扫描主机端口和服务来防止可能的漏洞。当发现主机受到攻击之后，应立即分析可能的漏洞，并加以预防，及时通知网络管理人员注意。

5.2.1.4　故障报告撰写要点

网络出现故障问题长期解决不了，就要建立一个单独文档记录所有的发现问题、解决问题的信息，这个问题档案的序号要记录到工作日志中以便交叉查询，项目结束后它应当记录了很多问题以及解决问题所需要的技术信息。

故障报告是反映网络系统出现故障情况及解决方法的文档，文档可以只是简单的文本形式，一页通常记录一个问题，也可以使用数据库，这样便于交叉查找。表 5.1 是故障报告的一个简单样本，建立它或使用它都非常节省时间。

项目结束后，这份文档要加入历史文档，供其他项目或其他组织使用。经常做这样的工作，测试的成本会随项目的不断进行而下降。

表 5.1　故障报告样本

故障报告
状态　　序号_____ 报告_____日期_____测试人_____日期_____ 修复_____日期_____测试人_____
关键操作参考：
故障描述：
故障解决：

5.2.2 典型例题分析

例 1 试述一般连接性故障排除的步骤。

分析：连接性故障可能发生在 OSI 7 层中的任何一个层次，在得到确认前，不要假定连接性的任何一个方面或者任何配置是正确无误的。其具体的步骤如下：

步骤 1：检查客户机和服务器上的 TCP/IP 地址和默认网关。可使用 ipconfig/all 命令。

步骤 2：确定客户机或服务器是否可以 ping 通它们的默认网关。

步骤 3：确认客户机是否可以 ping 通服务器的 TCP/IP 地址和主机名。

步骤 4：如果 IP 地址可以 ping 通但用主机名却 ping 不通，则可能是名称解析问题。

步骤 5：如果客户 ping 通服务器，但无法和应用建立连接，则可能服务器应用服务未启用。

通过以上步骤的推断，不难找到故障所在，然后进行恢复。

答案：从近到远逐一检查与连接有关的设备，确定故障位置，然后排除故障。

例 2 阅读以下说明，回答问题 1~2，将解答填入答题纸对应的解答栏内。(2004 年下半年下午试题四)

【说明】

网络解决方案如图 5.6 所示。该网络原先使用的是国外品牌的交换机，随着网络规模的扩大，增添了部分国产品牌的交换机，交换机 1 至交换机 5 均是国产 10M~100M 自适应交换机，交换机 6 和交换机 7 是第三层交换机。

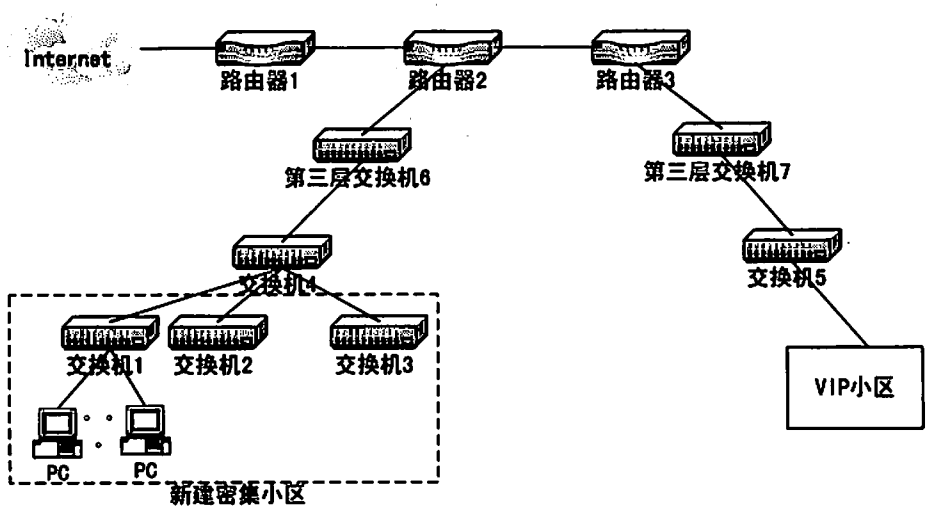


图 5.6 网络解决方案

该网络在运营过程中曾出现了下列故障：

故障 1

使用“网络故障一点通”测试新建密集小区用户和第三层交换机 6 之间的最大吞吐量，发现这些用户带宽都不超过 10Mb/s。

使用“在线型网络万用表”串联在第三层交换机 6 和交换机 4 之间，测试数秒钟后，发现它们之间的传输速率也是 10Mb/s。

故障 2

故障现象：VIP 小区用户不能上网，但能 ping 通路由器地址。

分析：由于 VIP 小区用户配置的是静态 IP 地址，而且处在同一网段，共用路由器上的一个地址作为网关地址。用户能 ping 通路由器，说明从用户到路由器间的路径是通的，因此需重点检查路由器。

操作过程如下：

首先，在路由器上，观察接口状态，未见异常。

然后，用 show ip route 观察 ① 表，未见异常。

最后，再用 show arp 观察 ② 表，发现路由器的 MAC 地址与工作人员以前保存在该表中的 MAC 地址不同，而是 VIP 小区中某个用户的 MAC 地址。

【问题】

1. 造成故障 1 的原因是什么?如何解决?
2. (1) 将故障 2 中①和②两处合适的答案填入答题纸相应的解答栏内。

(2) 故障 2 如何解决?

分析：根据测试结果可知交换机 4 和 6 之间的带宽为 10Mb/s，而由于交换机 1 和 4 都是自适应交换机，因而可以判断第三层交换机 6 的端口带宽最高为 10Mb/s，故解决此问题的简单方法就是将交换机 6 的端口升级，比如升级为 100M 端口，这样可以提升 PC 机访问速率。

对于第 2 个故障，关键在于了解访问互联网的过程。在网络中存在多种标识主机的方法，包括域名、IP 地址和 MAC 地址，对于同一台主机来说，它们应该是一致的，即具有一一对应的关系。而其中 MAC 地址是网络接口卡的物理地址，可以惟一确定一台主机，其他名称均可以改变。本题的故障在于 IP 地址与 MAC 地址的对应关系弄错了，因而无法找到正确的路由器接入互联网。解决的办法是修改 ARP 表中路由器 1 对应的 IP 地址与 MAC 地址的对应关系。

另外还需要掌握查看故障时常用的 show 命令的用法。

答案：

1. 交换机 6 的端口是 10M 端口，可以升级为 100M 端口。
2. (1) ①IP 路由表 ②ARP 表。

(2) 重新修改 ARP 表中的路由器 MAC 地址。

例 3　相邻办公室向管理员告知建筑物的电路不稳定，在同一时间客户又抱怨说网络瘫痪了。网络检查表明所有的用户都是直接连接在 Hub 上的，Hub 连接在 Cisco 路由器上，在本地连接的路由器上用“show interface”命令显示如下结果：

```
Router>show interface e0
Ethernet 0 is down, line protocols is down
```

这个问题应该如何描述?

分析：在日常维护中，简单的松散连接或物理线路的拼接经常发生。网络已经工作了一段时间，在路由器上，如果配置了不正确的协议封装，网络一开始就不能正常的工作，如果接口已经禁用了 administratively down，而不只是“瘫痪”，集线器端口故障会导致网络瘫痪，但同时接口不会瘫痪，因为路由器端口并不会受到影响。

答案：路由器与 Hub 间的网络线缆被拼接了。

例 4 在 FDDI 网络上，如果协议分析器记录显示一个较高的冲突数量，请问是什么原因？

分析：阻塞从来不会发生在令牌环网络上，这可能会发生在 100Mb/s 以太网络的通信量超过最大阈值的 30%的时候，在 FDDI 网络中是不会出现的，因为如果一个 FDDI 网络中的网卡坏了，这个网络将发生封装，以减轻问题信息的严重性。应该知道，令牌环网络一次只允许一个站点传输数据。

答案：冲突不可能发生在令牌环上，因此，协议分析器给出的报告是错误的。

例 5 在远程网络中，怎样禁止主机与工作站进行通信？

分析：工作站不使用 AS 直接与路由器交流路由信息，路由器将使用默认网关使路由器能够分发包到远程的目的地址。

如果这个工作站有一个不正确网关或没有默认网关，它将不能把包分发到路由器；如果这个路由器不含远程网络的路由信息，它将不能将这个包分发到远程目的地址；如果一个工作站的 IP 地址不正确，它将不能和路由器进行正常的通信；如果一个工作站的子网掩码不正确，它就会错误地认为远程网络在本地网络上，因此这个包不会分发到路由器上。

答案：路由器不包括路由到远程网络的表项，工作站错误设置 IP 地址，错误设置子网掩码，错误设置或没有默认网关等都可能导致工作站无法访问远程主机。

5.2.3 同步练习

在两个公司网站之间建立一条租用(DDN)线路连接时遇到如下问题：

过去这两个网站是通过 ISDN 线路使用 DDR 来连接的，由于信息量的增加，选用 256Kb/s 的租用线路更加合算。连接方式如图 5.7 所示。

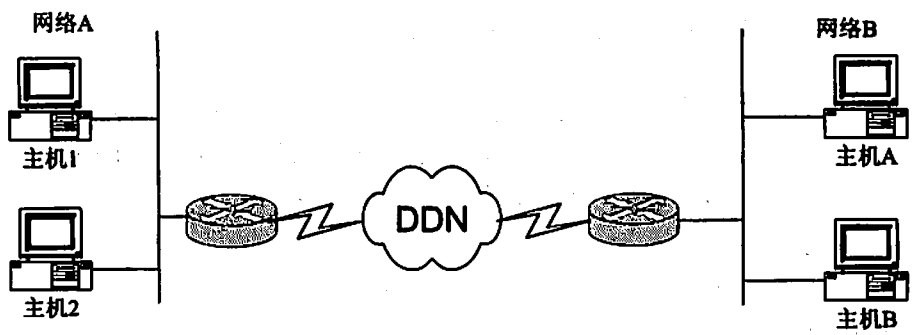


图 5.7 线路连接方式

现在决定为每个路由器配一个 NAN 串口网卡，提供 DB-60 串口，以便连接到电话公司的网络终端(NTU)上。电话公司来到两个网站进行了实地观察，并且安装了 NTU。先将两个网站的路由器的 DB-60 与 V.35 电缆相连接，然后开始进行路由的配置。建立这个配置后，两个路由器上的串口都不能运行，它们显示为无法工作的状态。

(1) 如果假定最初的配置有问题，用什么命令可以检查?

(2) 当检查完配置后发现并没有问题，然后决定按照 OSI 模型的顺序来进行系统的问题诊断。首先观察路由器的物理接口和 NTU，那么可以根据 NTU 的指示灯的哪个状态来判断它是正常的?

(3) 判断 NTU 正常后，如果想查看连接到路由器上的 DB-60 串口的电缆的状态，哪个命令可以查看这个状态?

(4) 路由器与 DB-60 串口连接电缆的状态如下所示，根据这两个输出找出问题所在。

```
HD unit 0,idb=0x96138,driver structure at 0x9A600
Buffer size 1524 HD unit 0,V.35 DCE cable
Cpb=0x21,eda =0x4940,cda=0x4800
RX ring with 16 entries at 0x214800
...
```

5.2.4 同步练习参考答案

(1) 应当用 show running-config 命令查看当前路由器的配置文件。

(2) NTU 的灯应当是绿色的。

(3) show controllers。

(4) 在这两个输出中，电缆显示的状态都是 V.35 DCE，而这里需要的是 V.35 DTE 电缆。将它们修改成 DTE 电缆后，串口将立即恢复为 Interface Up，Protocol Up 状态，这时就能够使两个网站之间的线路进行通信了。

5.3 危害安全的对策

5.3.1 考点辅导

5.3.1.1 危害安全情况分析

风险分析是安全管理系统需要提供的一个重要功能。它要连续不断地对网络中的消息和事件进行检测，对系统受到侵扰和破坏的风险进行分析。风险分析必须包括网络中所有有关的成分。

进行风险分析的一个方法是构造威胁矩阵，显示各个部分潜在的非攻击性或攻击性威胁。表 5.2 给出了一个威胁矩阵的例子。

非攻击性威胁包括：

- 盗听通话 目的是识别通话双方，获取秘密信息。

- 盗听数据　目的是获取口令等秘密信息。
- 分析业务流　获取业务量特征，以便进一步进行侵扰破坏。

表 5.2　威胁矩阵示例

威胁对象		非攻击性威胁			攻击性威胁				
		盗听通话	盗听数据	分析业务流	重复信息	修改信息	插入信息	伪造身份	拥塞网络
端点用户		H	M	L	H	H	H	H	H
交换机	电缆	M	M	M	M	M	M	M	M
	光缆	L	L	L	L	L	L	M	M
本地网	电缆	L	L	M	L	L	M	M	M
	光缆	L	L	L	L	L	L	M	M
长途网	电缆	H	H	H	H	H	H	M	H
	微波	H	H	H	H	H	H	M	M
	光缆	L	L	L	L	L	L	M	L
	卫星	M	M	M	M	M	M	M	M
软件	操作系统	L	L	L	M	M	L	M	M
	数据库	L	L	L	M	M	M	M	M
	应用	M	M	M	H	H	H	H	H

注：表中 H 表示高度威胁，M 表示中度威胁，L 表示低度威胁。

在大多数情况下，非攻击性威胁是可以防范的，而攻击性威胁却不能完全防范，常常会引起较严重的后果。攻击性威胁包括：

- 阻延或重发　重复或阻延信息的传送，以迷惑和干扰信息的接收者。
- 插入或删除　插入或删除传输中的信息，使信息接收者产生错误的反应。
- 阻塞传输　通过播放大量的信息拥塞传输系统，阻止网络中信息的正常传送。
- 修改数据　对关键数据(如账号)进行修改，引起网络管理的混乱。
- 伪造身份　使用伪造的身份标识进入网络，访问无权访问的信息，进行非法操作。

网络可以采用的安全服务多种多样，但是没有哪一个服务能够抵御所有的侵扰和破坏，只能通过对多种服务进行合理的组合来获得满意的网络安全性能。网络安全服务是通过网络安全机制实现的。OSI 系统管理标准中定义了 8 种网络安全机制，它们是加密、数字签名、访问控制、数据完整性、认证、伪装业务流、路由控制以及公证。

网络管理系统提供的安全服务可以有效地降低安全风险，但它们并不能排除风险。

与故障管理相同，安全管理也要提供报警、日志和报告功能。该功能要以大量的侵扰检测器(可以由软件实现)为基础。在发现侵入者进入网络时触发报警过程，登录安全日志和向安全中心报告发生的事件。在报警报告和安全日志中，主要应包括以下信息：

- 事件的种类
- 发生的时间
- 事件中通信双方的标识符

- 有关的资源标识符
- 检测器标识符

5.3.1.2 防火墙技术

防火墙是一种特殊的设备(通常是一个路由器，也可能只是一台运行专用软件的 PC 机)，它有选择地过滤或阻塞网络间的流量。通常防火墙都是硬件和软件的结合(例如：路由器的操作系统和配置)，它可能位于两个互相连接的私有网络处，更常见的是在一个私有网络与一个公共网络(比如 Internet)连接处。图 5.8 是常见防火墙的示意图。

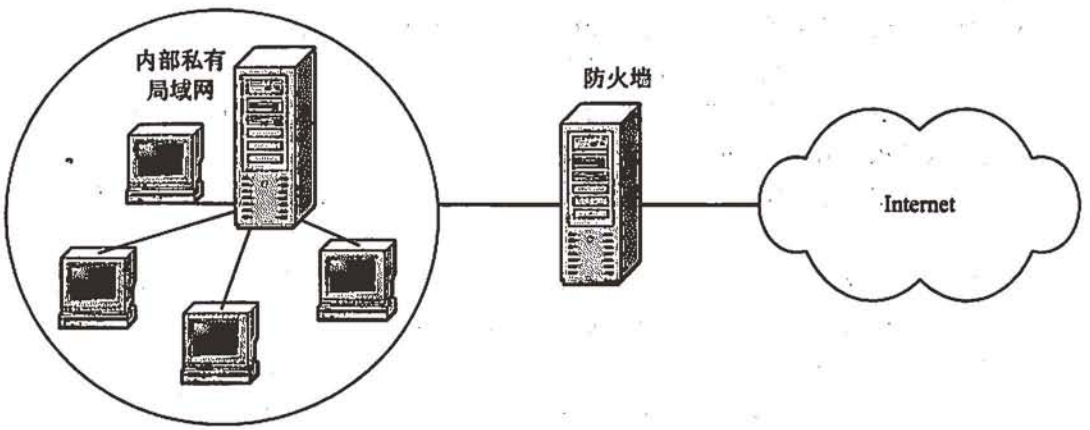


图 5.8 防火墙示意图

通过在网络中设置防火墙，可以过滤网络通信的数据包，对非法访问加以拒绝。系统设置防火墙后，可以为网络提供各种保护，主要包括以下几方面的内容：

- 隔离不信任网段间的直接通信。
- 隔离网络内部不信任网段间的直接通信。
- 拒绝非法访问。
- 地址过滤。
- 访问发起位置的判断。
- 过滤网络服务请求。
- 系统认证。
- 日志功能。

利用防火墙技术，通常能够在内外网之间提供安全保护。但是，仅仅使用防火墙保证网络安全还远远不够，这是因为：

- 入侵者可寻找防火墙背后可能敞开的后门。网络结构的改变，有时会造成防火墙上的安全策略失效。
- 入侵者可能就在防火墙内。在每个企业的内部网络中，每个内部网段上除连接着业务主机外，还有许多工作站，这些工作站与主机的通信不需要通过防火墙。如果攻击行为是从这些工作站上发起的，主机将处于无保护的状态。
- 由于性能的限制，防火墙不能提供实时的入侵检测能力。

单一应用防火墙技术，以上问题是不能得到有效解决的。但如果公司在重要主机上安

装实时入侵检测系统就可以解决由上述情况引起的安全问题。

5.3.1.3 入侵检测系统

入侵检测系统(IDS，Intrusion Detection System)可以弥补防火墙的不足，为网络安全提供实时的入侵检测及采取相应的防护手段，如记录证据、跟踪入侵、恢复或断开网络连接等。

1. 入侵检测系统的概念

(1) 基本概念

入侵行为主要是指对系统资源的非授权使用，可以造成系统数据的丢失和破坏、系统拒绝服务等危害。对于入侵检测而言的网络攻击可以分为 4 类：

① 检查单 IP 包(包括 TCP、UDP)首部即可发觉的攻击，如 winnuke、ping of death、land.c、部分 OS detection、source routing 等。

② 检查单 IP 包，但同时要检查数据段信息才能发觉的攻击，如利用 CGI 漏洞、缓存溢出攻击等。

③ 通过检测发生频率才能发觉的攻击，如端口扫描、SYN Flood、smurf 攻击等。

④ 利用分片进行的攻击，如 teadrop、nestea、jolt 等。

进行入侵检测的软件与硬件的组合就是入侵检测系统。入侵检测系统的原理图如图 5.9 所示。入侵检测通过对计算机网络或计算机系统中的若干关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

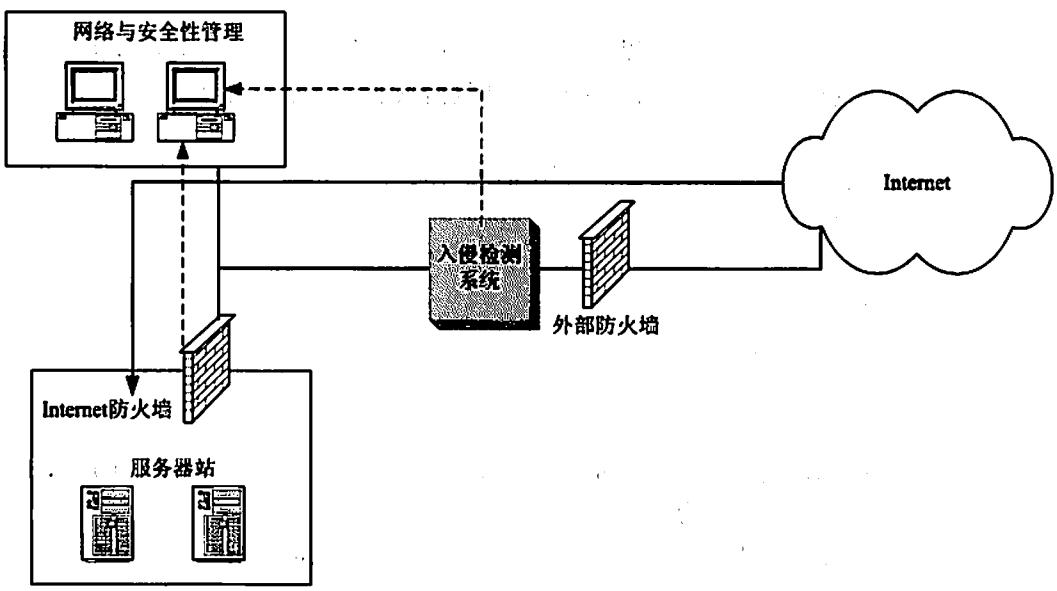


图 5.9 入侵检测系统的原理模型

(2) 任务

入侵检测系统执行的主要任务包括：监视、分析用户及系统活动；审计系统构造的弱点；识别、反映已知进攻的活动模式，向相关人士报警；统计分析异常行为模式；评估重要系统和数据文件的完整性；审计、跟踪管理操作系统，识别用户违反安全策略的行为。

(3) 步骤

入侵检测一般分为3个步骤，依次为信息收集、数据分析、响应(被动响应和主动响应)。

信息收集的内容包括系统、网络、数据及用户活动的状态和行为。入侵检测利用的信息一般来自系统日志、目录以及文件中的异常改变、程序执行中的异常行为及物理形式的入侵信息4个方面。

数据分析是入侵检测的核心。它首先构建分析器，把收集到的信息经过预处理，建立一个行为分析引擎或模型，然后向模型中植入时间数据，在知识库中保存植入数据的模型。数据分析一般通过模式匹配、统计分析和完整性分析3种手段进行。

入侵检测系统在发现入侵后会及时作出响应，包括切断网络连接、记录事件和报警等。响应一般分为主动响应(阻止攻击或影响进而改变攻击的进程)和被动响应(报告和记录所检测出的问题)两种类型。

2. 入侵检测系统技术

可以采用概率统计方法、专家系统、神经网络、模式匹配、行为分析等来实现入侵检测系统的检测机制，以分析事件的审计记录、识别特定的模式、生成检测报告和最终的分析结果。

发现入侵检测一般采用如下两项技术：

(1) 异常发现技术

异常发现技术假定所有入侵行为都是与正常行为不同的。它的原理是，假设可以建立系统正常行为的轨迹，所有与正常轨迹不同的系统状态则视为可疑企图。异常阈值与特征的选择是其成败的关键。其局限在于，并非所有的入侵都表现为异常，而且系统的轨迹难于计算和更新。

(2) 模式发现技术

模式发现技术是假定所有入侵行为和手段(及其变种)都能够表达为一种模式或特征，所有已知的入侵方法都可以用匹配的方法发现。模式发现技术的关键是如何表达入侵的模式，以正确区分真正的入侵与正常行为。模式发现的优点是误报少，局限是只能发现已知的攻击，对未知的攻击无能为力。

3. 入侵检测系统的分类

通常，入侵检测系统按其输入数据的来源分为3类：

(1) 基于主机的入侵检测系统 其输入数据来源于系统的审计日志，一般只能检测该主机上发生的入侵。

(2) 基于网络的入侵检测系统 其输入数据来源于网络的信息流，能够检测该网段上发生的网络入侵。

(3) 分布式入侵检测系统 能够同时分析来自主机系统审计日志和网络数据流的入侵检测系统，系统由多个部件组成，采用分布式结构。

另外，入侵检测系统还有其他一些分类方法。如根据布控物理位置可分为基于网络边界(防火墙、路由器)的监控系统、基于网络的流量监控系统以及基于主机的审计追踪监控系统；根据建模方法可分为基于异常检测的系统、基于行为检测的系统、基于分布式免疫的系统；根据时间分析可分为实时入侵检测系统、离线入侵检测系统。

4. 入侵检测的方法

入侵检测主要有以下几种方法：

(1) 静态配置方法

静态配置方法通过检查系统的当前系统配置，诸如系统文件的内容或者系统表，来检查系统是否已经或者可能会遭到破坏。静态是指检查系统的静态特征(系统配置信息)，而不是系统中的活动。

所以，静态配置分析方法需要尽可能了解系统的缺陷，否则入侵者只需要简单地利用那些系统中未知的安全缺陷就可以避开检测系统。

(2) 异常性检测方法

异常性检测技术是一种在不需要操作系统及其防范安全性缺陷专门知识的情况下，就可以检测入侵者的方法，同时它也是检测冒充合法用户的入侵者的有效方法。但是，在许多环境中，为用户建立正常行为模式的特征轮廓，以及确定用户活动的异常性报警的阈值的都是比较困难的事，所以仅使用异常性检测技术不可能检测出所有的入侵行为。

(3) 基于行为的检测方法

通过检测用户行为中那些与已知入侵行为模式类似的行为、那些利用系统中缺陷或间接违背系统安全规则的行为，来判断系统中的入侵活动。

入侵检测方法虽然能够在某些方面取得好的效果，但总体看来各有不足，因而越来越多的入侵检测系统都同时采用几种方法，以互补不足，共同完成检测任务。

5. 入侵检测系统的结构及标准化

(1) 结构

目前，通用入侵检测架构组织(CIDF)和 IETF 都试图对入侵检测系统进行标准化。CIDF 阐述了一个入侵检测系统的通用模型，将入侵检测系统分为 4 个组件：

① 事件产生器 CIDF 将入侵检测系统需要分析的数据统称为事件，它可以是网络中的数据包，也可以是从系统日志等其他途径得到的信息。事件产生器是从整个计算环境中获得事件，并向系统的其他部分提供此事件。

② 事件分析器 事件分析器分析得到的数据，并产生分析结果。

③ 响应单元 响应单元则是对分析结果做出反应的功能单元，它可以作出切断连接、改变文件属性等强烈反应，也可以是简单的报警。

④ 事件数据库 事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。

在这个模型中，前三者以程序的形式出现，而最后一个常是文件或数据流。入侵检测系统的几个组件常位于不同的主机上。一般会有 3 台机器，分别运行事件产生器、事件分析器和响应单元。

(2) 标准化

IETF 的 Internet 草案工作组(IDWG)专门负责定义入侵检测系统组件之间，以及不同厂商的入侵检测系统之间的通信格式，目前只有相关的草案(draft)，还未形成正式的 RFC 文档。IDWG 文档有 4 类：

① 入侵警报协议(IAP) 该协议是用于交换入侵警报信息、运行于 TCP 之上的应用

层协议。

② 入侵检测交换协议(IDXP)　这个应用层协议是在入侵检测实体间交换数据，提供入侵检测报文交换格式(IDMEF)报文、无结构的文本，二进制数据的交换。

③ IDMEF　是数据存放格式隧道文件 Tunnel，允许块可扩展交换协议 Beep，对等体能作为一个应用层代理，用户通过防火墙得到服务。

④ IAP　是最早设计的通信协议，它将被 IDXP 替换，IDXP 建立在 Beep 基础之上，Tunnel 文件配合 IDXP 使用。

6. IDS 与防火墙的比较

IDS 不同于防火墙的是，它是一个监听设备，没有挂接在任何链路上，无需网络流量流经它便可以工作。因此，对 IDS 的部署，惟一的要求是：IDS 应当挂接在所有所关注流量都必须流经的链路上。在这里，“所关注流量”指的是来自高危网络区域的访问流量和需要进行统计、监视的网络报文。在如今的网络拓扑中，已经很难找到以前的 Hub 式的共享介质冲突域的网络，绝大部分的网络区域都已经全面升级到交换式的网络结构。因此，IDS 在交换式网络中的位置一般选择在：尽可能靠近攻击源和受保护资源。这些位置通常是：服务器区域的交换机，Internet 接入路由器之后的第一台交换机，重点保护网段的局域网交换机等。两者不同点见表 5.3。

表 5.3　IDS 与防火墙功能比较表

比较项目	防 火 墙	IDS
设备类型	多穴主机，数据转发设备，完成类似于交换机和路由器的功能	一般单接口，数据采集、分析设备。
流量处理机制	过滤	无
对受检报文的操作	大量读写各层报文首部	仅拷贝
对链路速度的影响	取决于转发延迟	无影响
可附加模块	可实现网络层加密，应用层病毒检测、杀毒功能	不能实现加密、杀毒功能，但可以实现病毒检测功能
对入侵行为的处理	拒绝、报警、日志记录	报警、日志记录和有限反击
入侵检测的准确性	近于流量转发负载压力，对报文普遍检查，可能发生误报、漏报	无转发负担，有入侵知识库支持，误漏报率较低
对访问日志的记录	只作条目式记录，框架较粗	非常详细，包括访问的资源和报文内容等
设备稳定性对网络的影响	要求非常高，否则可能造成网络链路的阻断	无
应用层内容恢复	一般不提供，但可据此进行过滤和替换功能	能够完整修复应用层内容，能够对网络特定流量进行全程监视和记录，为管理员判断进攻者、收集证据提供了强有力手段。
对网络层以下各层的支持	由于对物理链路隔断，必须支持所有网络层以下的协议才能维持网络正常运作，如 RIP、OSPF、IGMP 等	不作要求

5.3.1.4 计算机病毒知识

1. 定义

计算机病毒(Computer Virus)在《中华人民共和国计算机信息系统安全保护条例》中定义，指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

2. 病毒的来源

主要是人为编制的，用来恶作剧、报复、自我保护、特殊目的、实验等。

3. 病毒的特点

破坏性、传染性、寄生性、潜伏性、可触发性等。

4. 病毒的分类

按照破坏性分为：良性病毒、恶性病毒。

按照工作原理分为：引导型、文件型、宏病毒、网络型、混合型。

5. 网络型病毒

网络中常见的病毒主要包括特洛伊木马、蠕虫病毒、脚本病毒等三种。

(1) 特洛伊木马

特洛伊木马是一种可执行程序，它伪装成一个正常的应用程序，诱使用户运行。但一旦用户运行了它，其就有可能破坏用户的系统和数据或者在用户的系统上开一个后门以控制用户的系统。

(2) 蠕虫病毒

蠕虫病毒是通过分布式网络来扩散传播特定的信息或错误，进而造成网络服务遭到拒绝并发生死锁。这种“蠕虫”程序常驻于一台或多台机器中，并有自动重新定位的能力。如果它检测到网络中的某台机器未被占用，它就把自身的一个拷贝(一个程序段)发送给那台机器。每个程序段都能把自身的拷贝重新定位于另一台机器中，并且能识别它占用的哪台机器。

(3) 脚本病毒

脚本病毒主要是利用软件或系统操作平台等的安全漏洞，通过执行嵌入在网页 HTML 超文本标记语言内的 Java 小应用程序 Applet、JavaScript、VBScript、ActiveX 部件和其他网络交互技术支持的可自动执行代码等，以强行修改用户操作系统的注册表设置及系统实用配置程序，或非法控制系统资源盗取用户文件，或恶意删除硬盘文件、格式化硬盘为行为目标的非法恶意程序。

6. 病毒的防治和清除

计算机病毒的出现和蔓延，已对计算机应用和社会生活构成严重威胁。因此必须认真地做好计算机病毒防治工作。一般认为病毒的防治应从三方面入手，包括加强思想教育、严格组织管理和加强技术措施，三者缺一不可。

计算机病毒亦应以预防为主，而预防计算机病毒，主要是堵塞病毒的传播途径。目前病毒的主要传播途径是通过计算机网络和软件。网络中的共享文件一旦感染上病毒，病毒就会快速传播到各个站点。隐藏病毒的软盘只要在无毒的机器上一经使用，该机的内存、

硬盘就会被感染而成为新的病源。为了防止病毒的传播，可以采取的措施是：

- 管理上应制定出严格的规章制度。
- 技术上应采取的对病毒的预防措施。

7. 网络防毒

所谓网络防毒，是指在全网范围内建立起一套全方位、具备实时检测能力的防病毒体系，实现从服务器到工作站再到客户端的全方位病毒防护和集中式管理。

与传统单机防毒不同的是，网络防毒体系需要统一管理、统一规划，管理者应对企业网结构了如指掌，细到了解内部服务器和客户机个数，进而能够通过可控的中央管理平台，统一安装客户端的防毒产品，掌握病毒发作情况、防毒产品狙击病毒的运行情况，管理各设备代码库更新工作等。具体来讲，网络防毒的管理模式有以下几种：

(1) 分散式管理模式

分散式管理模式是每一系列产品都有一个自己的管理平台，与其他系列的产品管理平台互不联系，只能一个管理平台管理一个系列的产品，管理平台是嵌入到产品内部的。这种管理模式适用于服务器较少的小型局域网，目前很多国内外厂商的防毒产品都采取这种模式。

(2) 直接集中控制管理模式

直接集中控制管理模式把所有系列的产品集中在一个单独设立的防毒服务器上进行分发和管理，这里典型的代表是 Symantec 控制中心(Symantec System Center，SSC)。Symantec 对于网络各层次的防毒产品是通过该控制中心为企业网络防毒的安装、维护、更新及报表等提供集中管理工具，其中防火墙、网关、Lotus Notes 以及 Microsoft Exchange 防毒产品均采用基于 Web 的管理方式，因此可以实现远程管理。这种管理模式比较适合于服务器较多的中型局域网。

(3) 既可分散又可集中控制的管理模式

在既可分散又可集中控制的管理模式方面最具代表性的是趋势科技，它的各系列防毒产品都各有一个内嵌式管理平台，而且都有适合远程管理的 Web 方式，而这一系列管理平台又交给另外一个独立的网络防毒管理平台 Trend Virus Control System (TVCS)来进行统一全面的管理。TVCS 让管理人员可以通过单一的主控台设定、监控以及管理网络上所有的防毒软件，超越了平台与地理上的限制。此外，它还能管理一些其他防毒厂商的产品。趋势科技防毒集中管理模式具有专业的管理功能，既适合于小型网络的分散式管理模式(不需要 TVCS)，又适合于大型跨网段、跨平台网络的集中管理。

5.3.2 典型例题分析

例 1 公司网络中的设备或系统(包括存储商业机密的数据库服务器，邮件服务器，存储资源代码的 PC 机，应用网关，存储私人信息的 PC 机，电子商务系统)哪些应放在 DMZ 中，哪些应放在内网中？并给予简要说明。(2004 年上半年下午试题一问题 4)

分析：当打算在网络上安装一个防火墙时，首先想到的可能就是把所有的客户和服务器都放到它的后面。这对于小企业来讲是一个较好的解决办法，但对于大企业，就应该考虑去构建一个叫做非军事区 DMZ(Demilitarized Zone)的周边安全网络，用来区分外网与

内网。

DMZ 是放置公共信息的最佳位置，这样用户、潜在用户和外部访问者都可以直接获得他们所需的关于公司的一些信息，而不用通过内网。公司中的机密的和私人的信息可以安全地存放在内网中，即 DMZ 的后面。DMZ 中的服务器不应包含任何商业机密、资源代码或是私人信息。DMZ 服务器上的破坏最多只可能造成在恢复服务器时的一段中断服务。

答案：DMZ 中放置邮件服务器、应用网关、电子商务系统。内网中放置机密数据服务器、存储私人信息的 PC 机和存储资源代码的 PC 机。DMZ 是放置公共信息的最佳位置，用户、潜在用户和外部访问者不用通过内网就可以直接获得他们所需要的关于公司的一些信息。公司中机密的、私人的信息可以安全地存放入内网中，即 DMZ 的后面。DMZ 中的服务器不应包含任何商业机密、资源代码或是私人信息。

例 2 将下列术语和定义进行正确匹配。

术语：

- 完整性破坏
- 机密性破坏
- 可用性破坏

定义：

- 网络无法处理大量数据的后果
- 攻击者更改敏感数据
- 很难被探测到

答案：

完整性破坏——攻击者更改敏感数据

机密性破坏——很难被探测到

可用性破坏——网络无法处理大量数据的后果

例 3 什么类型的威胁是针对整个网络的？

答案：针对整个网络的攻击包括：

- 侦察攻击　搜索网络以发现可能的目标。
- DOS 攻击　破坏与整个网络连接。
- 流量攻击　破坏通过网络的数据流，例如：更改网络中传输的数据。

例 4 身份验证的 3 种类型是什么？

分析：

身份验证需要确切知道对方拥有何种资源或知道何种信息，这就是身份验证的本质所在。

答案：验证传统上基于以下 3 种检验的一种：

- 对象知道某事
- 对象拥有某物
- 对象即为某物

例5 如何管理来自受害服务器的攻击?

答案：电子商务应用软件通常是多层排列并运行于多台服务器。将多层系统隔离成其自身的 DMZ 网络保证它们之间有一个防火墙系统，在前端破坏事件中保护更多的安全服务器。防火墙通常限制来自暴露电子商务服务器的连接，因此对其他主机的破坏可能性很小。局域网交换机访问控制机制(如虚拟网)可以隔离仅次于同一段上的主机。网络和主机入侵检测系统可以监视独立主机和子网，以检测攻击迹象并确定潜在的成功破坏。

5.3.3 同步练习

1. 为了保证足够的安全，网络系统的安全政策应该包括哪些内容?
2. 由网络操作系统提供的安全机制包括哪些?

5.3.4 同步练习参考答案

1. 包含下列内容：口令政策、软件安装政策、机密和敏感数据政策、网络访问政策、电子邮件使用政策、互联网使用政策、调制解调器使用政策、远程访问政策；与远程场所、互联网、客户以及卖主网络相连接的政策；使用手提式电脑和贷方机器的政策；机房访问政策等。安全政策应当向用户清楚地解释他们能做什么和不能做什么，以及这些措施如何保证网络的安全。

2. 不论网络是运行在 Novell、Microsoft 操作系统之上，还是 Unix 操作系统之上，均可以通过对用户分类进行限制来实现基本的安全机制。

公共权限，其包括浏览和执行服务器提供的程序，以及在一个共享数据目录中读、创建、修改、删除和执行文件的权限。

除此之外，网络管理员需要根据用户的安全级别对用户分组，并且对不同的组分配相应的附加权限以满足这些组的需求。

除了限制用户对服务器上文件和目录的访问权限，网络管理员也可限制用户访问服务器和资源的方法。包括时间段、登录的总时间、源地址、不成功登录尝试次数等。

5.4 本章小结

网络管理是对计算机网络的配置、运行状态和计费等进行的管理。它提供了监控、协调和测试各种网络资源以及网络运行状况的手段，还可提供安全管理和计费等功能。

本章讲述网络管理技术、网络管理功能和协议、网络管理系统以及网络日常管理和维护。

复习时应着重掌握网络管理的基本功能，包括配置管理、性能管理、故障管理、安全管理和计费管理等。另外还需要掌握网络管理协议 SNMP 和 MIB-II 的有关知识，以及常用的网络监控工具的使用方法，并掌握对网络的性能、故障、安全等监控的基本方法。

第 6 章　网络系统的评价

大纲要求：

- 系统评价　系统能力的限制，潜在的问题分析，系统评价要点。
- 改进系统的建议　系统生命周期，系统经济效益，系统的可扩充性，建议改进系统的要点。

6.1　网络系统的评价

6.1.1　考点辅导

6.1.1.1　系统评价

1. 系统评价的基本概念

网络系统的评价也要遵循一般系统评价原则，下面就简要介绍系统评价的基本概念、评价尺度、评价任务和评价步骤。

(1) 系统评价

所谓系统评价，是指根据预定的系统目的，在系统调查和可行性研究的基础上，主要从技术和经济等方面，就各种系统设计的方案所能满足需要的程度及消耗和占用的各种资源进行评审，选择技术上先进、经济上合理、实施上可行的最优或满意的方案。根据评价与系统的关系，可以区分出如表 6.1 所示的评价类型。

表 6.1　系统评价的类型

序号	评价与系统的关系	评价的类型
1	评价与决策	决策前丨中丨后评价
2	评价与系统发展过程	事前丨中丨后评价
3	评价信息特征	基于数据丨模型丨专家知识的评价；综合评价

在系统开发过程中，通过系统工程的思想、程序和方法的应用，可以提出许多开发系统的可选方案，这时就要通过系统评价技术从众多的可选方案中找出最优的方案。然而，要决定哪一个方案最优却未必容易。

(2) 价值

所谓价值，就是评价主体(个人或集体)对某个评价对象(如待开发的系统、待评价的方案等)的认识(主观感受)和估计。

价值是评估主体主观感受到的，是人们对客观存在的事物从各种各样的分析中主观抽象出来的。价值不是孤立地附属于某一评价对象，因此也就没有衡量价值的绝对尺度(标准)。

(3) 评价尺度

系统评价是由评价对象、评价主体、评价目的、评价时期、评价地点等要素构成的一个综合性问题。因此，对评价技术来说，就是首先引进和确定评价尺度(标准)，然后通过评价尺度，对评价对象进行测定，并确定其价值。

常用的评价尺度大致可分为四种：第一种称为绝对尺度，即规定原点尺度不变。第二种称为间隔尺度，有些场合只要求测得数值差才有意义。第三种是顺序尺度，它可以用顺序或反映顺序的字符来表示，这时需要的只是其顺序关系。最后一种是名义尺度，这仅仅是为了识别或分类需要而用数字与对象相对应。如学校的班级编号和运动员的编号等就是这种名义尺度。

在评价中，要根据评价的目的和评价对象的性质来确定评价尺度。

(4) 系统评价的任务

系统评价的主要任务就在于从评价主体根据具体情况所给定的、可能是模糊的评价尺度出发，进行首尾一致的、无矛盾的价值测定，以获得对多数人来说均可以接受的评价结果，为正确决策提供所需的信息。由此可见，系统评价和决策是密切相关的。为了在众多替代方案中做出正确的选择，就需要有足够的丰富的信息，其中包括足够的评价信息。所以说，系统评价只有和方案决策和行为决策联系起来才有意义。评价是为了决策，而决策需要评价，决策过程需要评价过程。

(5) 系统评价的步骤和构成

如图 6.1 所示，系统评价的一般步骤包含：评价问题、评价系统分析(前提条件探讨)、评价资料的搜集、评价指标的选择、评价函数的确定、评价价值的计算和综合评价等几个阶段。

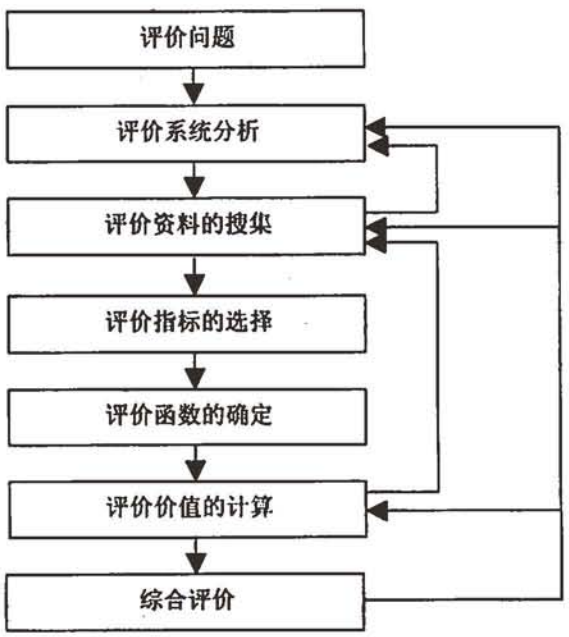


图 6.1　系统评价步骤

2. 系统评价要点

系统评价的要点包括评价系统分析、评价资料的搜集、评价指标的选择、评价函数的确定、评价价值的计算和综合评价等。

(1) 评价系统分析

在正式进行系统评价前，有必要对评价系统进行分析，探讨和明确一系列前提条件，这是做好系统评价的首要工作，主要包括：

① 评价的目的。总体来说，评价的目的是为了更好地决策，但具体来说，评价目的又大致可分为以下4个方面：

- 使评价系统达到最优 为了使系统结构或技术参数达到最优，有必要量化评价系统各种替代方法的价值。
- 对决策的支持 当评价者或决策者在选择最优方案的过程中，对替代方案的各自价值感到迷惑不解时，评价提供的信息可供决策参考。
- 决定行为的说明 对于复杂的问题即使做出合理的决定，如果没有评价或评价过程模糊不清，也会遭到人们的怀疑、误解以至抵制，所以，为了形成统一意志，需要有某种程度的客观评价。
- 问题的分析 评价的过程往往是问题分析的过程。有许多问题利用相关的评价方法可以把复杂的问题分解成简单的小问题，再通过对这些小问题的分析和评价，获得系统的综合评价。

② 评价系统范围的界定。它主要是确定系统的边界，即评价对象涉及多大范围。评价系统的范围不应过小，以免忽略重要影响部门而有失系统性；同时也不应过大，以免使评价问题过度复杂化。

③ 评价的立场。在进行系统评价时必须明确评价主体的立场，即明确评价主体是系统使用者还是开发者抑或是第三者等，这对于以后评价方案的确定、评价项目的选择等都有直接的影响。

④ 评价的时期。即系统评价处于系统开发全过程的哪个时期(评价时期一般可分为事前评价、事中评价和事后评价)。

⑤ 评价系统环境的分析。系统环境的分析是指对存在于系统外的物质的、经济的、信息的影响因素进行分析，以了解这些因素对评价系统的影响。系统环境可能受到的影响可分为三大类：技术的、经济的及社会的影响。

(2) 评价资料的搜集

对评价系统的功能、费用、时间及使用寿命进行预测和估计，为确定评价尺度、评价函数等搜集评价所需资料。

(3) 评价指标的选择

评价指标的选择是评价目标与实际情况共同决定的，具体选择应注意以下几点：

① 评价指标必须与评价目的和目标密切相关。

□ 评价指标应当构成一个完整的体系，即全面地反映所需评价对象的各个方面。

□ 评价指标总数应当尽可能地少，以降低评价负担。

(4) 评价函数的确定

评价函数是使评价定量化的一种数学模型。不同问题使用的评价函数可能不同，同一个评价问题也可以使用不同的评价函数，因此，对选用什么样的评价函数本身也必须做出评价。一般应选用能更好的地达到评价目的的评价函数或其他适应的评价函数。

评价函数本身是多属性、多目标的。尤其当评价目的在形成统一意见或进行群体决策时，对确定评价函数会产生不同的看法。因此，在对系统实施进行之前，应该在有关人员间进行充分的无拘束的讨论，否则难以获得有效的评价。

(5) 评价价值的计算

当评价函数确定后，评价尺度也随之而定。在评价价值计算之前，还需要确定各评价项目的权重。总之，评价尺度和评价项目的权重应保证评价的客观正确性和有效性。

(6) 综合评价

综合评价就是对系统进行技术、经济、社会等各方面的全面评价。但综合评价的各个方面和评价项目不能一概而论，应根据具体评价对象而定。以企业开发新产品为例，一个完整的综合评价体系大致包括以下几个方面：经营管理方面、技术方面、市场方面、时间方面、经济方面、体制方面和社会方面等。

安排定期的系统评价被确定为网络系统实施过程实现后鉴定的一部分。定期的系统评价安排在系统实现后3个月，但不能超过一年。评价小组负责审定下列内容：

- 系统效率
- 系统有效性
- 解决周期
- 响应时间
- 信息的关联
- 输入输出的分配及控制
- 输入输出的格式和内容
- 文件、记录和数据库的结构
- 更新和后备措施
- 系统资料的通用性

关于需要进一步改进的不足之处和建议都要编制成文件，并提交给相应业务领域的管理人员。

3. 系统能力的限制

网络系统的主要功能是资源共享和数据传输，因而系统的能力具体体现在服务器处理能力和传输能力，也即媒体的带宽和中继设备的交换能力。由于每种设备的配置是固定的，因而其处理能力也有一定的范围限制，若传输媒体带宽固定，其单位时间内的传输能力也有一定限制，另外还要考虑利用率的问题。因此在系统评价时应该确切地了解系统的设备配置及其性能，对即将开放的网络服务进行评估，考查是否超出网络系统的能力，如果不能满足则不应该接受，采取其他措施扩容或者限制网络用户的应用，以保证网络系统正常可靠地运行。

4. 潜在的问题分析

系统设计实施完成后，需要对整个系统进行评估，即要考查系统的功能、性能、可靠性、可用性、安全性等方面是否达到设计目标，需要分析各个方面是否存在潜在的问题隐患，为网络系统的维护和升级提供依据。

(1) 网络性能问题分析

使用多种性能监视工具对包括带宽、利用率、吞吐量、系统延时等在内的关键性能指标进行监控并记录结果，与基准线进行比较，观测系统性能出现波动的时间和周期并分析其原因。

(2) 网络安全性问题分析

从网络系统外部进行分析，考察计算机网络基础设施中防火墙的安全性。

从网络系统内部进行分析，考察网络系统内部计算机的安全性。

从网络应用系统进行分析，考察每台硬件设备运行的操作系统的安全性。

使用专用软件进行分析，查找存在的安全漏洞和隐患并提出解决方案。

(3) 网络可靠性问题分析

与有关专家一道全面分析网络的可靠性，包括物理方面、逻辑方面的可靠性及其健康运行性，评估系统与需求的相合性，如果不相合则存在差距，还应该考虑到网络系统运营后新的应用需求及其增长带来的影响，预期未来几年内网络可靠性存在的问题，写入评估报告。

(4) 形成问题报告

网络系统分析人员整理已经收集完整的各方面的评估报告，进一步分析找出系统存在的各方面问题，形成全面的问题报告，问题报告中应该详细描述问题存在的原因、发生的相关环境及对应用可能存在的影响，提交给上一层决策者，用于在系统升级时的参考依据。

6.1.1.2 改进系统的建议

1. 系统生命周期

开发一个新的网络系统或修改一个已有的网络系统的过程称为网络的生命周期。网络的生命周期体现的是一个新的网络或新特征的构思计划、分析设计、实施运行和维护的过程，这个过程在修改之后又要重新开始。这种生命周期与软件工程中的软件的生命周期非常类似。

虽然目前没有哪个生命周期可以完美地描述所有的项目开发，但是网络流程周期和网络循环周期这两种基本的生命周期模型得到了软件工程师的认可和应用。下面针对这两种网络生命周期进行介绍。

(1) 网络流程周期

网络流程周期由分析、设计、实施、测试和运行等 5 个不同的阶段组成，生命周期又叫做一个流程，因为每一项工作是从一个阶段“流到”下一个阶段，正如图 6.2 所描绘的那样。当系统正常运行以后，网络生命周期就会由于更新而重新开始。

按照这种模型开发网络，在开始下一个阶段之前，前面的每个阶段的工作必须已经完成。一般情况下，不允许返回前面的阶段，如果出现前一阶段的工作没有完成就开始进入下一个阶段，则会造成工期拖延，随之将带来严重的超支。

网络流程周期的主要优势在于所有的计划在较早的阶段完成。该系统的所有负责人对系统的具体情况以及工作进度都非常清楚。这有助于较早地知道工期和更容易地协调工作。

网络流程周期的缺点是比较死板，不灵活。因为在项目完成之前，用户的需求往往会发生变化，这使得已开发的部分需要经常修改，从而影响工作的进程。网络流程周期适用于开发很小的项目。

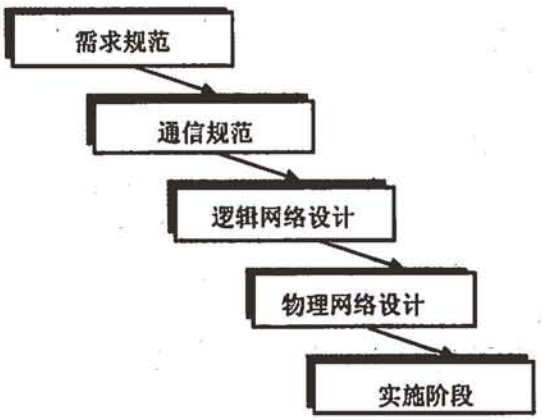


图 6.2　网络流程周期

(2)　网络循环周期

网络循环周期又称为网络漩涡周期，是从网络流程周期演变而来。其出现的目的是克服网络流程周期在灵活性方面的缺点。

变化管理是网络循环周期的指导性原则。与网络流程周期不同的是，网络循环周期能够快速适应新的需求，这可以通过几次重复所有阶段来实现，每次循环将产生一个新的循环周期，它由以下 4 个阶段组成，图 6.3 是网络循环周期的示意图。

网络循环周期是一个连续体，通过在网络设计中的每一个循环实现最终性能的一个子集，用户就有机会在项目完成之前反馈他们的意见和建议并在新的一轮循环中加以考虑，新的性能被加入，用户提出的问题随之得以解决。

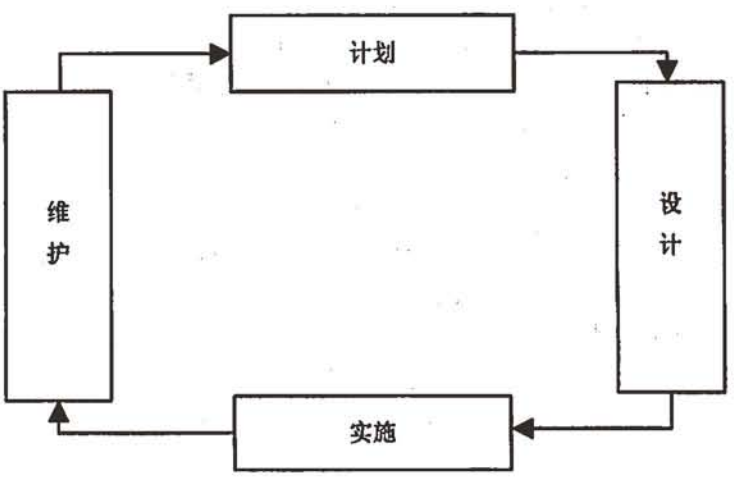


图 6.3　网络循环周期

虽然网络循环周期在处理需求变化方面比网络流程周期优越，但也有其自身的缺点，这就是无法预知用户以后会要求什么，这样就很难估计出最终的经费和完工日期。最糟的是，按照网络循环周期模型开发网络，很容易陷入无休止的更新循环中。

2. 系统经济效益

付出应当有所得，而且应当大大地超出付出，这是市场经济的基本原则，因此，网络系统评价的另一个重点是投资/效益分析。投资分析参见技术可行性的结果，效益分析包括经济效益和社会效益两部分。经济效益进一步划分为直接经济效益和间接经济效益两部分。

直接经济效益指通过本项工程的实施所产生的可见的经济效益。例如：使用自动化处理和电子化传输技术可以节省日常的邮政费用、差旅费开支等。

间接经济效益指通过本项工程的实施所产生的间接经济效益，例如：节省人力、提高自动化程度、提高功效及加快部门内或者部门间的信息交互等。

对于经济效益分析，应当尽可能地考虑各个方面，并进行量化，包括：节省了多少时间、节省了多少人力和工作量，相当于创造多少产值。例如：使用办公自动化，减少了人工录入的工作，不仅节省了人力，还降低了录入差错的可能性，以及避免由此而引起的问题。

需要指出的是，在分析投资/效益比时，也应当对投资风险进行分析。事实上，进行任何投资活动时，必然地存在着某种风险。一味地描述效益而忽略可能的风险是不明智的。投资风险主要体现在如下方面：实际投资值超过估计值；应用效果比预期的差；效益比预期的低；出现不可预测的意外或环境变化。在可行性分析时，应当考虑各种投资风险的可能性，并提出降低风险的措施，亦即可行性分析应当客观地反映所有的问题。

社会效益是指通过本项工程的实施，在人员素质的提高方面、通过自动化管理在社会上产生的影响，包括对国内其他同类机构的影响等。

3. 系统的可扩充性

可扩充性是满足所有网络通信流量的需求并随着公司的发展能够容纳更多通信流量的一种能力。可扩充性涉及网络设计的几个方面。如以校园网为例，需要考虑的方面包括：

- 计算机工作站将要使用到的重要的服务器资源放在何处。
- 使用的网络技术能否支持放置在每个楼层的所有工作站。
- 连接校园网的主干网能否支持全校所有的工作站间的跨建筑通信量。
- 集线器和交换机是否有足够的带宽能力处理各楼层和建筑物间的通信量。
- 网络协议是否能够正确地对环境里的每台工作站进行寻址。
- 局域网环境能否容纳广播站的容量。
- 网络两个最远节点间的距离是否超出了所用网络技术允许的范围。
- 网络是否存在有特别高要求的工作组，对它们如何处理。

可扩充性是在网络规划设计阶段就应该考虑的问题，在网络设计中，应该保留一定的扩展空间，以备以后网络升级之用，但随着系统的运行和升级，可扩展性将逐步丧失，因此在网络系统升级时也应该考虑这个问题，以便长久的保持系统可扩充的能力。

4. 建议改进系统的要点

网络系统正常运行后，经过网络管理人员长时间对系统性能、安全、可靠性、可用性、

可扩充性等方面的观察和数据积累，系统出现的问题会越来越清晰地显示在面前。如：

- 安全漏洞和安全隐患
- 性能瓶颈
- 可靠性措施不力
- 可用性不符合需求
- 扩充空间有限，不能满足今后应用

根据对系统存在问题的分析并参照潜在问题分析的报告，可以针对每个问题改进方案，以使整个网络更加安全可靠的运行。

6.1.2　典型例题分析

例　系统的响应时间如何计算？影响响应时间的因素有哪些？如何缩短响应时间？

分析：对一个网络环境下的信息查询系统进行网络延时测量可以分为以下 3 步：

(1) 测量在本地进行查询的响应时间。

(2) 通过网络在远地进行同样的查询，测量其响应时间。

(3) 上述两次测量的结果之差即为网络延迟，对于传送一个文件的响应时间可用下述公式计算：

$$R = A + (P \times S)$$

式中：R 为响应时间；A 为存取时间(例如，在源节点和目的节点之间建立网络连接所需的时间)；P 为对每个数据块进行处理、存取磁盘以及在链路间传送文件所需的时间(秒)；S 为文件大小，以数据块为单位。

测量拷贝一个空文件所需的时间可得到 A 的值。用以下方法可得到 P 的值：

(1) 测量传输不同大小文件所需的时间，得到响应时间和文件大小的函数关系，如图 6.4 所示。

(2) 在图 6.4 中选择不同文件大小的两点(S_1 和 S_2)，以及对应的传输时间(t_1 和 t_2)。

(3) 按下式求得 P：

$$P = (t_2 - t_1)/(S_2 - S_1)$$

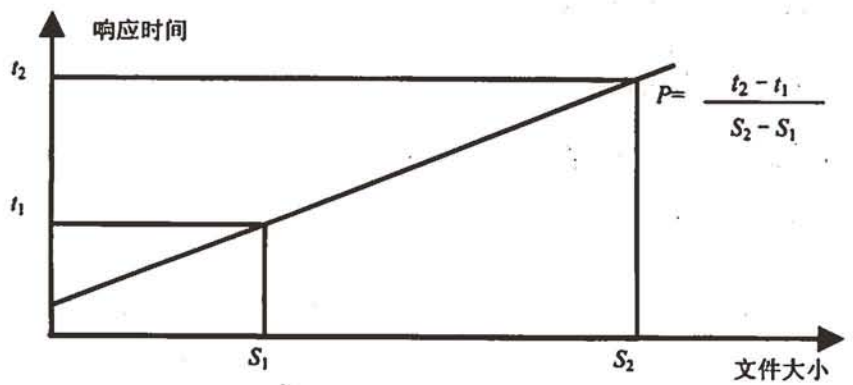


图 6.4　响应时间和文件大小的关系

影响响应时间的因素来自3个部分，即源节点、网络和目的节点。

- 源节点　即本地系统的处理。
- 网络　即传输部分。
- 目的节点　即远程系统的处理。

一般来说，响应时间取决于在这三个部分处理通信数据的元件特性、源节点和目的节点的负载以及网上的通信量。

在源节点和目的节点影响响应时间的因素有：

- CPU的容量以及可给网络使用的时间。
- 系统的类型，如分时系统或专用系统。
- 在源节点的终端线速度。
- I/O处理能力。
- 缓冲器大小。
- 报文大小。
- 内存访问优先调度和存取速度。

在网络层，影响响应时间主要有以下3个因素：

- 协议处理的开销。
- 通信密度即网络负载。
- 传输时间。

此外，网络的规模、网络拓扑的复杂性、路由器的容量、传输误差和重传机制、交换系统特性等都对响应时间有影响。

为了改善响应时间这一网络特性，可以将网络硬件和网络资源升级，但要花费代价。

有时可采取更为简单的方法，通过调整负载、调整应用以及实现分布处理等方法来改善网络响应时间。

答案：略。

6.1.3 同步练习

1. 常见的评价理论主要有哪几种？
2. 常见的评价方法有哪几种？
3. 评价的目的是什么？

6.1.4 同步练习参考答案

1. 常见的评价理论主要有5种：

(1) 效用理论

这里的效用理论与经济学中的效用理论一样，效用只是主观的评价，根据效用并利用效用函数来进行定量的分析和评价，一般来说，这种方法比较方便。但是效用数值的大小只表示顺序尺度，本身没有意义。效用理论是以评价主体个人的价值观为基础而建立起来的数学理论，其中包含了许多假定，因此不能原封不动地运用到实际中去。效用理论是评价理论的基础。

(2) 确定性理论

确定性理论主要是用统计的方法使评价数量化，这时需要收集足够数量的、质量相等的数据，同时要有能看透问题本质的敏锐的洞察力。评价数量化在数据选择方面变化不可预见，这一点是与自然科学和工程学问题不同的地方。因而碰到质的问题数量化，首先必须了解评价的目的，洞悉问题的实质。其程序是：在确认使用统计方法的妥当性和有效性后，收集适当数据，以统计方法确认假定，并在数据通过检验后，能够在一定程度上建立起数量化评价模型，进行属性评价或综合评价。

(3) 不确定理论

不确定理论使评价处于迷惑不解的困境，多数情况是发生在含有不确定因素的决策当中。但如果已经掌握事件发生的概率，则可以用期望值作为评价函数，以便作为确定性理论来处理。即使在缺乏数据的情况下，也可凭借专家的经验和直观判断，以及以往发生的概率，对事件发生的可能性做出定量估计。

(4) 非精确理论

除了事件发生的不确定性以外，还有的人认识所固有的非精确性(模糊性)。为了进行这种评价，需要利用模糊集理论。

(5) 最优化理论

评价对象的数学模型本身也可能成为评价函数，如数学规划方法就是一个典型的例子。

2. 常见的评价方法有以下 5 种：

(1) 费用-效益分析

费用-效益分析是系统评价的经典方法之一。在经济学理论中，要求从经济总体上考虑费用和效益的关系，已达到资源的最优化分配。实现这种方法的困难在于如何正确地测定效益，以及如何估计长期投资和效益的社会折现率。采用这种方法的问题是，仅仅从经济观点考虑效益，不能从社会观点考虑效益。为了弥补这方面的不足，后来又有了有效度观点和费用-有效度分析的概念。

(2) 关联矩阵法

关联矩阵法应用于多目标系统。它是用矩阵形式来表示各替代方案有关评价项目的平均值。然后计算各方案评价值的加权和，通过分析比较，评价值加权和最大的方案即为最优方案。应用关联矩阵法的关键在于确定各评价指标的相对重要度(即权重)，以及由评价主体给定的评价指标的评价尺度。

(3) 关联树法

关联树法是作为一种有助于对复杂问题进行评价的方法而产生的。最初它是用来对国家战略性的技术预测和设计的评价，后来在开拓市场、投资分析等不确定状态下进行评价时也广泛应用起来。关联树法进行评价时的工作主要包括三部分：第一部分是分析和评价系统的目的及达到目的所需的技术或方法之间是如何联系起来的。其重点是关联树建立，并通过关联树来评价。第二部分是分析由于对某部分问题的解决而促进另一部分问题解决的相互影响效果，并据此修正关联树。第三部分是根据开发能力和现状与目标作比较，以选择开发时机等。

(4) 层次分析法

层次分析法作为一种评价方法，和上述的关联矩阵法和关联树法属于同一类型。层次

分析法是一种定性分析和定量分析相结合的评价决策方法，它将评价者对复杂系统的评价思维过程数学化。其基本思路是评价者通过将复杂问题分解为若干层次和若干要素，并在同一层次的各要素之间简单地进行比较、判断和计算。就可以得出不同替代方案的重要度，从而为选择最优方案提供决策依据。层次分析法的特点是：能将人们的思维过程数学化、系统化，便于人们接受；所需定量数据信息较少。但要求评价者对评价问题的本质、包含要素及其相互之间的逻辑关系能十分透彻地掌握。这种方法尤其可用于对无结构特性的系统评价以及多目标、多准则、多时期等的系统评价。

(5) 模糊评价法

模糊评价法是运用模糊集理论对系统进行综合评价的一种方法。通过模糊评价，能获得系统各替代方案优先顺序的有关信息。模糊评价法也是常用的一种综合评价方法。

3. 总体来说，评价的目的是为了更好地决策，但具体来说，评价目的又大致可分为4个方面：

(1) 使评价系统达到最优。为了使系统结构或技术参数达到最优，就有必要量化评价系统各种替代方法的价值。

(2) 对决策的支持。当评价者或决策者在选择最优方案的过程中，对替代方案的各自价值感到迷惑不解时，评价提供的信息可供决策参考。

(3) 决定行为的说明。对于复杂的问题即使做出合理的决定，如果没有评价或评价过程模糊不清，也会遭到人们的怀疑、误解以至抵制，所以，为了形成统一意志，需要有某种程度的客观评价。

(4) 问题的分析。评价的过程往往是问题分析的过程。有许多问题利用相关的评价方法可以把复杂的问题分解成简单的小问题，再通过对这些小问题的分析和评价，获得系统的综合评价。

6.2 本 章 小 结

网络系统评价一般属于事后评价，即在网络系统建成后进行评价。本章主要介绍了网络系统评价的意义、评价理论、评价方法、评价内容及在网络生命周期中的重要作用。关键要掌握网络系统评价的要点和步骤，及对网络系统维护和升级的重要意义。

第7章 网络协议

大纲要求：

- 商用网络协议(SNA/APPN，IPX/SPX，AppleTalk、TCP/IP)。
- 商务协议(XML，CORBA，COM/DCOM，EJB)。
- Web服务(WSDL，SOAP，UDDI)。

7.1 商用网络协议

7.1.1 考点辅导

7.1.1.1 SNA/APPN

SNA(Systems Network Architecture)，是IBM公司制定的网络体系结构。SNA是IBM大型机和中型机的主要联网协议，在IBM主机环境中得到广泛的应用。

SNA设计的主要目的是端到端的通信，以及让用户应用程序远离复杂的数据通信系统，使用户感觉到数据通信系统的透明性。端用户通常是一台终端或者是主机上的应用程序。SNA网络就是为端用户提供相互之间通信的服务。

SNA网络由物理部分(physical components)和软件部分(software components)组成。物理部分由处理器、通信控制器和终端控制器组成，物理部分通过数据链路、电话连接、微波等方式连接起来。软件部分由访问方式(ACF/VTAM，高级通信操作程序/虚拟远程通信访问法)、应用子系统(CICS，用户信息控制系统)、IMS(因特网多播服务)、用户应用程序和网络控制程序(ACF/NCP，高级通信操作程序/网络控制程序)构成。

SNA提供一种以主机为中心的通信架构，定义了一些逻辑部件以实现通信功能。LU(Logical Unit)用来处理端到端的通信；PU(Physical Unit)在SNA节点上用来管理物理资源；SSCP(System Services Control Point)是网络的访问控制中心；DLC(Data Link Control)用来管理数据传输的链路；PC(Path Control)用来处理数据在SNA网络中传输的路由控制。

1. SNA协议结构

SNA参考模型与OSI相类似，SNA分层结构与OSI分层结构对比如图7.1所示，SNA也具有7个协议层。

下面介绍分别各个协议层：

(1) 物理链路控制层(Physical Link Control Layer)

物理链路控制层提供多种不同类型的物理连接，包括电缆、光纤和卫星等多种通信模式。在有些情况下，它还允许两点间有多个不同的连接，这让用户可以指定传输的详细类型，类似于Internet协议提供的服务类型。此层还可被用来将长串数据分割为单独的单元，

并分别传输。除了主机和前端处理器(代表主机处理请求的特殊处理器)间可使用并行传输，一般传输都使用串行链路传输。节点互联的介质有铜线、光纤电缆或微波等。

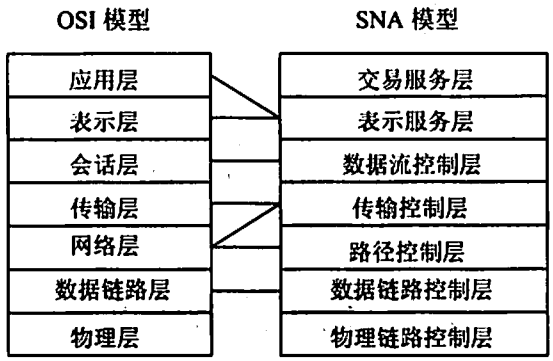


图 7.1 OSI 分层结构与 SNA 分层结构对比

(2) 数据链路控制层(Data Link Control Layer)

数据链路控制层负责在网络内的物理连接之上提供可靠的数据传输。它的功能包括定义帧格式，进行差错控制和流控制。

数据链路控制层支持各种不同的网络协议实现，例如，同步数据链路控制(SDLC)规程、二进制同步通信(BISYNC)协议、IEEE 802.5 令牌环网(IBM token-ring Network)、X.25 和 IEEE 802.2 逻辑链路控制协议、帧中继(Frame Relay)和光纤分布式数据接口(FDDI)。其中同步数据链路控制规程对 SNA 网络中帧的流动进行数据链路层上的控制。

数据链路控制层为路径控制层提供统一的接口。

(3) 路径控制层(Path Control Layer)

路径控制层提供了控制路由选择的功能，并可以细分数据报以及重装数据报以适应传输设施，负责提供和正确的数据分解有关的排序服务。

(4) 传输控制层(Transmission Control Layer)

传输控制层提供了面向连接的服务，在两端点之间建立一条监视数据流和确保传送的链路。

(5) 数据流控制层(Data Flow Control Layer)

数据流控制层提供监视数据流并处理两个端点间的会话以防止数据溢出的服务。

(6) 表示服务层(Presentation Services Layer)

表示服务层执行数据转换，并提供应用程序接口。

(7) 交易服务层(Transaction Services Layer)

交易服务层为应用程序提供了到网络服务的接口。

2. SNA 的扩展——APPN

高级对等网络(Advanced Peer to Peer Networking，APPN)是 IBM 为了对抗 TCP/IP 的威胁，将 SNA 与 TCP/IP 网络连接起来，在 1985 年作为流行的客户机/服务器计算技术的替代物提出的。它允许两个主机之间建立 SNA 连接。APPN 是一个对等的路由选择协议，支持点对点通信和分布式客户端/服务器通信。APPN 用来处理对等节点间建立的会话、动态透明路由计算和为高级程序间通信(APPC)业务赋予业务优先级等。

例如，PC 主机访问在使用高级程序间通信(APPC)会话的大型机上运行的应用，可以使用 APPN 实现物理单元(PU)和逻辑单元(LU)之间的通信，两者都是网络寻址单元(NAU)的一种形式，用于控制主机和终端的通信过程。LU 代表着 SNA 端节点，如用户或应用的连接；PU 则是硬件设备或终端，两个 LU 通过关联着的 PU 进行通信。SNA 网络环境中使用了许多种类型的 LU 和 PU。

APPN 在保持主机系统的多样性的同时也提供了一个企业范围内的非集中网络计算。在 APPN 网上，大小型系统相互对等操作。IBM 的策略是在包容工业标准协议(例如，TCP/IP 和 OSI 协议)的同时继续支持 APPN。这个思想已在联网方案中表示出来，多协议传输网(Multi Protocol Transmission Network，MPTN)就是一个例子，它使应用程序从底层众多网络协议中解脱出来，允许编写与一种特定协议一起工作的应用程序来使用其他协议。使用 IBM 的多协议传输网络就能把 AS/400 同那些支持常见的 PC 协议(如 TCP/IP 和 IPX 的令牌环网或以太网)连接起来。

7.1.1.2　IPX/SPX

IPX/SPX(Internetwork Packet eXchange/Sequences Packet eXchange，网际包交换/顺序包交换)是 Novell 公司的通信协议集。与 NetBEUI(网络基本输入输出系统增强型用户接口)的明显区别是，IPX/SPX 显得比较庞大，在复杂环境下具有很强的适应性。因为，IPX/SPX 在设计一开始就考虑了多网段的问题，具有强大的路由功能，适合于大型网络使用。当用户端接入 NetWare 服务器时，IPX/SPX 及其兼容协议是最好的选择。但在非 Novell 网络环境中，一般不使用 IPX/SPX。尤其在 Windows NT 网络和由 Windows 95/98 组成的对等网中，无法直接使用 IPX/SPX 通信协议。

IPX/SPX 及其兼容协议不需要任何配置，它可通过“网络地址”来识别自己的身份。Novell 网络中的网络地址由两部分组成：标明物理网段的“网络 ID”和标明特殊设备的“节点 ID”。其中网络 ID 集中在 NetWare 服务器或路由器中，节点 ID 即为每个网卡的 ID 号。所有的网络 ID 和节点 ID 都是一个独一无二的“内部 IPX 地址”。正是由于网络地址的惟一性，才使 IPX/SPX 具有较强的路由功能。

在 IPX/SPX 协议中，IPX 是 NetWare 最底层的协议，它只负责数据在网络中的移动，并不保证数据是否传输成功，也不提供纠错服务。IPX 在负责数据传输时，如果接收节点在同一网段内，就直接按该节点的节点 ID 将数据传给它；如果该接收节点是远程的(不在同一网段内，或位于不同的局域网中)，数据将交给 NetWare 服务器或路由器继续下一步传输。SPX 在整个协议中负责对所传输的数据进行无差错处理，所以 IPX/SPX 也叫做 Novell 的协议集。

Windows NT 中提供了两个 IPX/SPX 的兼容协议：NWLink IPX/SPX 兼容协议和 NWLink NetBIOS，两者统称为“NWLink 通信协议”。NWLink 协议是 Novell 公司 IPX/SPX 协议在微软网络中的实现，它在继承 IPX/SPX 协议优点的同时，更适应了微软的操作系统和网络环境。Windows NT 网络和 Windows 95/98 的用户，可以利用 NWLink 协议获得 NetWare 服务器的服务。如果你的网络从 Novell 环境转向微软平台，或两种平台共存时，NWLink 通信协议是最好的选择。不过在使用 NWLink 协议时，其中的 NWLink IPX/SPX 兼容协议类似于 Windows 95/98 中的 IPX/SPX 兼容协议，只能作为客户端的协议实现对

NetWare 服务器的访问，离开了 NetWare 服务器，此兼容协议将失去作用；而 NWLink NetBIOS 协议不但可在 NetWare 服务器与 Windows NT 之间传递信息，而且能够用于 Windows NT、Windows 95/98 相互之间任意通信。

7.1.1.3 AppleTalk

AppleTalk 网络体系结构是苹果计算机公司在 20 世纪 80 年代开发并不断完善的局域网络协议簇，这种网络利用 Apple 机的打印机端口相连接。AppleTalk 遵循 OSI 模型，最多可连接 32 个节点。在 AppleTalk 网络中，打印机是网络上的一个节点，它利用 AppleTalk 通信协议和 Apple 计算机沟通。

AppleTalk 当前有 Phase1 和 Phase2 两个版本。Phase1 协议支持一个物理网络，只有一个网络号驻留在一个区域中，现在已经过时。现在 AppleTalk 发布的产品是 AppleTalk Phase2，Phase2 协议支持单个物理网络上的多个逻辑网络，允许网络存在于多个区域。

AppleTalk 是每台 Macintosh 机内建的网络通信协议。这意味着每台 Macintosh 机都带有这种网络能力。AppleTalk 是分布式客户/服务器网络系统的一个早期实现版本，支持对等模式通信。AppleTalk 网络体系结构与 OSI 模型结构的对应关系如图 7.2 所示。

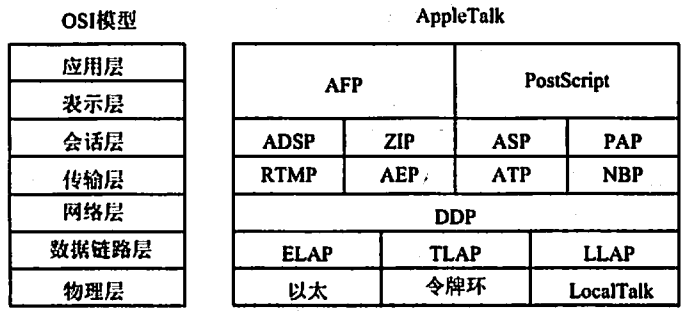


图 7.2 AppleTalk 网络体系结构与 OSI 模型结构的对应关系图

(1) 应用层协议

AppleShare 协议是 Apple 机上的通信协议，它允许计算机从服务器上请求服务或者和服务器交换文件。AppleShare 可以在 TCP/IP 协议或其他网络协议(如 IPX、AppleTalk)上进行工作。使用它时，用户可以访问文件、应用程序、打印机和其他远程服务器上的资源。它可以和配置了 AppleShare 协议的任何服务器进行通信，Macintosh、Mac OS、Windows NT 和 Novell Netware 都支持 AppleShare 协议。

(2) 表示层协议

AppleTalk 文件协议(AppleTalk Filing Protocol，AFP)执行 AppleTalk 协议簇中表示层和应用层的功能。

AFP 用于 AppleShare 网络中服务器和客户机之间的通信，允许 AppleTalk 工作站通过网络共享 AppleShare 服务器上的文件和应用程序，支持通过网络来恢复和存储文件。

AFP 协议允许用户采用与操作本地存储文件相同的方式操作远程存储文件，从而保持网络的透明性。在这个过程中，AFP 利用 ASP、ATP 提供的服务。

(3) 会话层协议

AppleTalk 会话协议(AppleTalk Session Protocol，ASP)对应 OSI 模型的会话层，在客户

机、服务器间建立和维护会话。ASP 是一个不对称协议，客户端初始化会话、发送命令到对话的另一边。ASP 也提供了一种方法使服务端可以发送命令到客户端，例如，文件服务器可以通过消息系统通知所有客户端本文件服务器即将关闭。ASP 被 AFP 用来使用户可以操作一个远端文件服务器上的文件。

AppleTalk 数据流协议(AppleTalk Data Stream Protocol，ADSP)是一个面向连接的协议，支持会话层基于 socket 的应用程序及进程通过 AppleTalk 完成全双工的数据流交换。

AppleTalk 区域信息协议(Zone Information Protocol，ZIP)提供应用程序及进程访问区域名称的服务。网络上的每个节点都属于一个区域。区域名称用来标识属于某个部门或地区的节点组。ZIP 协议使用应用程序及进程可以访问：本节点的区域的名称、本地网络上的所有区域的名称、Internet 上的所有区域的名称。

(4) 传输层协议

AppleTalk 回应协议(AppleTalk Echo Protocol，AEP)是两个 AppleTalk 节点之间连通性的一种测试，其中一个节点发送一个包给另一个节点并在响应中接收回应或拷贝。

AppleTalk 事务协议(AppleTalk Transaction Protocol，ATP)使两个套接字(socket)之间能可靠地进行事务处理，其中一个请求另一个执行一项给定的任务并报告结果。ATP 同时抓住请求和响应，保证请求/响应对无丢失交换。

AppleTalk 名称绑定协议(Name Binding Protocol，NBP)提供给应用程序和进程利用映射的名称代替网络号和地址访问计算机。

AppleTalk 路由选择表维护协议(Routing Table Maintenance Protocol，RTMP)提供一种 AppleTalk 互联网管理路由表的方法，决定如何将数据包从一个 socket 转发到目标网络。RTMP 实现在一个路由器维护路由表找到可能的最短路径。在 AppleTalk 工作站上只包括 RTMP 的一小部分，叫做 RTMP 桩。

(5) 网络层协议

AppleTalk 数据封包传输协议(Datagram Delivery Protocol，DDP)做为无连接协议在 socket 间以离散包的方式传输数据到目标地址。DDP 提供最有效的传输，但不保证发送的包被正确地送达目标。

7.1.1.4 TCP/IP

TCP/IP(Transmission Control Protocol/Internet Protocol)协议是 Internet 最基本的协议，简单地说，就是主要由底层的 IP 协议和 TCP 协议组成的。

1. TCP/IP 参考模型

按照 TCP/IP 协议，将 Internet 分为五个层次，也称为互联网分层模型或互联网分层参考模型。这五个层次分别是应用层(第五层)、传输层(第四层)、网络层(第三层)、数据链路层(第二层)、物理层(第一层)。具体模型如图 7.3 所示。

- 物理层　对应于网络的基本硬件，是 Internet 的物理构成，例如，PC 机、互联网服务器、网络设备等。物理层对这些硬件设备的电气特性作了一个规范，使这些设备都能够互相连接并兼容使用。
- 数据链路层　定义了将数据组成正确帧的规范和在网络中传输帧的规范。帧是指一串数据，是数据在网络中传输的基本单位。

- 网络层　定义了在 Internet 中传输的“信息包”的格式，以及从一个源通过一个或多个路由器到达最终目标的“信息包”转发机制。
- 传输层　为两个用户进程之间建立、管理和拆除可靠而又有效的端到端连接。
- 应用层　定义了应用程序使用 Internet 的规范。

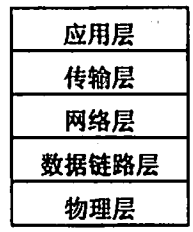


图 7.3　TCP/IP 协议模型

2. TCP/IP 主要协议

下面将介绍在网络层、传输层、应用层中使用的 TCP/IP 主要协议。

(1) 网络层

TCP/IP 网络层包括以下协议：

IP(网间协议)——定义一套在网络中通信的规则。IP 包括地址信息和一些控制信息。IP 有两个主要任务：在网络中提供无连接的、尽力而为的数据报传送，以及提供数据报分片和重组以支持具有不同最大传输单元(MTU)的数据链路。IPv4 是当前网络中使用的版本；IPv6 是新的协议版本。

ARP(地址解析协议)——允许主机动态地发现对应于特定 IP 网络层地址的 MAC(传输媒体访问控制)地址。给定网络中的两个设备若要通信，它们必须知道对方设备的物理地址。

RARP(逆地址解析协议)——用于将 MAC 地址映射到 IP 地址。未知其 IP 地址的无盘工作站在启动时可使用 RARP，它在逻辑上是 ARP 的逆过程。RARP 依赖于具有 MAC 地址到 IP 地址映射表项的 RARP 服务器。

ICMP(网际控制报文协议)——用以将错误以及其他有关 IP 分组处理的信息报告给源站。

(2) 传输层

TCP/IP 传输层中定义了以下两个传输层协议：

TCP(传输控制协议)——提供 IP 网络中面向连接的、端到端的可靠数据传输。TCP 使用三次握手机制建立连接。三次握手通过允许各方对初始序列号达成一致来使得连接两端同步。此机制也保证了各方已准备好数据发送/接收，并且知道对方也已准备好。使用此机制保证会话建立期间和会话终止后不会传输或重传分组。

UDP(数据报协议)——作为 IP 和上层进程接口的无连接协议。与 TCP 不同，UDP 并未给 IP 加入可靠性、流量控制或差错恢复等功能。由于 UDP 的简单性，UDP 头比 TCP 包含更少的字节，同时消耗更少的网络开销。

TCP 和 UDP 使用协议端口号来相互区分运行在同一设备上的多个应用。端口号是 TCP 和 UDP 段的一部分，用来识别数据段属于哪个应用。众所周知的或标准的端口号被分配给各种应用，以使得 TCP/IP 协议的不同实现可以互操作。这些众所周知的端口号的例子包括

以下几种：

- FTP(文件传输协议)　TCP 端口 20(数据)和端口 21(控制)。
- Telnet　TCP 端口 23。
- TFTP(普通文件传输协议)　UDP 端口 69。

(3) 应用层

在 TCP/IP 协议中，对应 OSI 模型的上面三层并成一层，称为应用层。这里有许多应用层协议，它们代表多种应用，主要包括以下几种：

- FTP(文件传输协议)和 TFTP(普通文件传输协议)　用于传输大量数据。
- SNMP(简单网络管理协议)　用于网络管理，报告网络异常，并设置网络阈值。
- SMTP(简单邮件传输协议)　提供电子邮件服务。
- DNS(域名系统)　将网络节点名转换成网络地址。

7.1.2　典型例题分析

例 1　简述 TCP 窗口机制。

分析：TCP 的特点之一是提供体积可变的滑动窗口机制，支持端到端的流量控制。TCP 的窗口以字节为单位进行调整，以适应接收方的处理能力。处理过程如下：

(1) TCP 连接阶段，双方协商窗口尺寸，同时接收方预留数据缓存区。

(2) 发送方根据协商的结果，发送符合窗口尺寸的数据字节流，并等待对方的确认。

(3) 接收方根据当前的处理能力，调整接收窗口的尺寸，并在确认中告知发送方。

(4) 发送方根据确认信息，改变窗口的尺寸，增加或者减少发送未得到确认的字节流中的字节数。调整过程包括：如果发送拥塞，发送窗口缩小为原来的一半，同时将超时重传的时间间隔扩大一倍。

(5) TCP 的窗口机制和确认保证了数据传输的可靠性和流量控制。

答案：略。

例 2　分别描述 IP 协议和 TCP 协议所提供的服务。

分析：IP 协议提供不可靠的、尽力的、无连接的数据投递服务。

(1) 不可靠的投递服务

IP 协议无法保证数据报投递的结果。在传输的过程中，数据报可能会丢失、重复、延迟和乱序等，但是 IP 服务的本身却不关心这些结果，也不将这些结果通知收发双方。

(2) 无连接的投递服务

每个数据报独立处理和传输，因此，由一台主机发出的数据报序列，可能取不同的路径，甚至其中的一部分数据报会在传输过程中丢失。

(3) 尽力的投递服务

IP 协议软件决不简单地丢弃数据报，只要有一线希望，就向前投递；尽力投递的另一种体现方法是 IP 协议软件执行数据报的分段，以适应具体的传输网络，数据报的合段则由最终节点的 IP 模块予以完成。

TCP 协议在 IP 协议软件提供的服务基础上，支持面向连接的、可靠的、面向流的投递服务。

(1) 面向流的投递服务

应用程序之间传输的数据可被视为无结构的字节流(或位流)，流投递服务保证收发的字节顺序完全一致。

(2) 面向连接的投递服务

流传输之前，TCP 收发模块之间需建立连接(类似虚电路)，其后的 TCP 报文在此连接基础上传输。TCP 连接报文通过 IP 数据报进行传输，由于 IP 数据报的传输导致 ARP 地址映射表的产生，从而保证了后继的 TCP 报文可以具有相同的路径。

(3) 可靠的投递服务

发送方 TCP 模块在形成 TCP 报文的同时，形成一个所谓的“累计核对”。“累计核对”类似校验和，并随同 TCP 报文一起传输。接收方 TCP 模块根据该校验和判断传输的正确性。如果传输不正确，接收方简单地丢弃该 TCP 报文，否则进行应答。发送方如果在规定的时间内未能获得应答报文，将自动进行重传动作。

答案：略。

7.1.3 同步练习

1. 请列举一些面向连接的协议。
2. 请列举一些路由协议。
3. Novell 网络中的网络地址由哪两部分组成?
4. IP 地址有哪几种分配方式?
5. 解释 SNA 节点(SNA node)的概念。

7.1.4 同步练习参考答案

1. SMTP，FTP，Telnet，ATM，AppleTalk，TCP。
2. RIP(路由选择信息协议)、IGRP(内部网关路由选择协议)、EIGRP(增强 Internet 网关路由选择协议)、OSPF(开放最短路径优先)、BGP(外部网关协议)。
3. 标明物理网段的“网络 ID”和标明特殊设备的“节点 ID”。
4. 静态(固定)分配和动态分配。
5. 在 SNA 协议结构中，由数据链路连接起来的物理部分(SNA physical components)被称之为 SNA 节点(SNA node)。SNA 节点有两种：子域节点(subarea nodes)和外围节点(peripheral nodes)。

7.2 商 务 协 议

7.2.1 考点辅导

7.2.1.1 XML

XML(可扩展标记语言)是 SGML(标准通用标记语言)的一个优化子集。SGML 是 ISO(国

际标准化组织)在 1986 年推出的一个用来创建标记语言的语言标准。SGML 为出版业提供了一种将数据内容与显示分离开来的数据表示方法，使得数据独立于机器平台和处理程序。SGML 的确在许多大型出版系统中很有用，但是它的复杂性使其难以直接应用到 Internet 上，而 HTML 是专为 Web 上发布超文本而设计的标记语言，它是用 SGML 定义标记语言的一个典型例子，但是 HTML 本质上主要关注 Web 浏览器如何在页面上安排文本、图像和按钮等，过多地考虑外观使其缺乏对结构化数据的表示能力。另外，HTML 中有限的标记不能满足很多 Web 应用的需要，如基于 Web 的大型出版系统和新一代的电子商务，而为各种应用需要不断地往 HTML 中增加标记显然不是最终的解决方法，究其原因是 HTML 缺乏可扩展性。解决方案应该是简化 SGML 使之能应用到 Web 上。在此背景下，作为 Web 上使用的 SGML 的一个优化子集，XML 应运而生。

同SGML类似，XML是一种元标记语言，使用者可按需创建新的标记，XML的可扩展性就在于此。带标记的元素是XML文档的构造块，这种元素可以有若干个属性，并可以包含零个或多个子元素。这些子元素可以是文本数据，也可以是带标记的元素。

XML 文档可以在它的文档类型声明(Document Type Declaration)里声明某个 DTD (Document Type Definition，文档类型定义)。DTD 是关于 XML 文档中出现的标记和元素结构的语法约束，可用来验证一个 XML 文档。DTD 是一系列关于元素类型(Element Type)、属性(Attributes)、实体(Entities)和符号(Notations)的定义。它定义了文档所需的标记，比如可在文档里使用的元素类型，这些元素之间可能的联系。

由于 DTD 缺乏对 XML 文档的内容及其语义的约束机制，这将限制 XML 处理器进行有效的类型检验，应用软件开发者将不得不专门编写有关类型检验的代码。因此有必要为 XML 建立一个更全面的有效性约束机制，使 XML 处理器更好地进行有效性检验。这样就产生了 XML Schema Language。用 XML Schema Language 书写的 XML 文档定义了相应 XML 文档的规则，以约束其数据元素及其关系。首先，Schema 文档从数据结构和数据类型两方面更严格地约束了相应的 XML 文档，它可以定义 DTD 所无法定义的规则，而 DTD 仅从结构上对 XML 文档进行有限的约束。其次，DTD 语言有其独立的语法形式，而 XML Schema Language 实际上是 XML 语言的一个应用(类似 HTML 与 SGML 语言的关系)，因此，Schema 文档本身就是一个 XML 文档，可以用 XML 工具进行分析，这样 Schema 文档也就可以用现有的 DTD 语言加以描述。

1. XML 和 HTML 的区别

SGML，XML，HTML 这三种标记语言的相互关系可以描述为：XML 是 SGML 的一个子集，而 HTML 是 SGML 的一个具体应用实例，同样，HTML 也是 XML 的一个应用实例，具体地来说，HTML 是由 XML 或 SGML 定义出来的。目前，XML 已经开始被广泛地采用，并且得到越来越多的数据库、Internet 软件厂商的支持。XML 在 Web 应用的实现方面可以取代 HTML，主要是源于 XML 和 HTML 的以下本质区别：

(1) HTML 是面向表示的，而 XML 是面向内容的。于是，XML 文档就更多地反映了文档的内容和逻辑结构信息；而 HTML 只能反映在表示上表现出来的一部分结构信息，而且这些结构信息是脱离内容的。

(2) HTML 的标注(tag)是有限的，而 XML 的标注是可扩展的。要使用 HTML 有限的标注来表示复杂的内容是不可能的；而使用 XML，用户可以自定义标注，来表示自己想要

表示的内容及其结构。

(3) HTML 文档不能提供任何关于整个文档内容、结构的信息，除非扫描整个文档；而 XML 文档可以通过提供 DTD 或是 XML Schema 文档来说明文档的可能的限制结构。于是，XML 文档可以提供更多的关于内容的模式(Schema)信息。

(4) HTML 是 Web 显示数据的通用方法，而 XML 提供了一个直接处理 Internet 数据的通用方法。HTML 着重描述 Web 页面的显示格式，而 XML 着重描述的是数据的内容及其结构，更深层次地看，描述的是 Internet 上共享交换的内容。

由于 XML 和 HTML 有着本质上的不同——XML 比 HTML 提供了更多的对于内容和结构的说明和限制的机制，使得存储、查询、管理 XML 文档相对而言更容易。总之，XML 使用一个简单而又灵活的标准格式，为基于 Web 的应用提供了一个描述数据和交换数据的有效手段。HTML 描述了显示全球数据的通用方法，而 XML 提供了直接描述处理全球数据的通用方法。

2. XML 的主要特点

XML 是一种自描述的数据共享机制，其主要特点如下：

- 自描述性 这个特性使差异性可以存在，使计算机可以在没有人为干涉的情况下，理解数据的含义。
- 可扩展性 文档通过 DTD 或 XML Schema 来定义文档结构，使其他信息系统能自动了解文档的内容。
- 可校验性 用户可以通过 DTD 或 XML Schema 来校验 XML 文档的格式是否满足 DTD 或 XML Schema 的约束。
- 层次结构 能够保证信息的层次性描述。例如，一个商品可以有商品名、商品代码和价格，价格又可以有基本价格、商品税和运输费等。
- 丰富的链接定义 对应于 HTML 单一的单向单通道链接，XML 提供各种不同的链接，如一对多、多对一和双向链接。
- 多样的样式表支持 XML 把数据内容与它们的表现形式分开。这样既可以只关心数据的逻辑结构，也可以通过样式表来格式化数据的表现。甚至可以定义自己的个人样式表来显示各种不同的 XML 数据。

3. XML 的应用

随着 XML 在 Internet 应用中的不断普及，XML 从 Web 网站的内容管理、内容描述起步，逐渐发散到其他众多基于 Internet 的应用中。这些所有 XML 相关的应用主要如下：

(1) 内容管理发布

依靠 XML 的可自定义可扩展的能力来描述整个 Web 世界上种类繁多、样式丰富多彩的数据内容，依靠一次描述、多次表现的 XML 标准应用模式使得基于 XML 的内容能够以多种形式进行信息发布。这些发布方式包括 Web 网站内容发布、电子出版内容发布以及其他出版业内容发布等。

(2) 电子商务应用

在这个领域中，XML 一般承担了以往 EDI(电子数据交换)所承担的角色，依靠 XML 来描述交换商务事务信息，实现分布式的电子商务应用的交互。由于 XML 是可定制的和

可扩展的，人们制定了很多用于特定领域的商务事务信息描述规范。

(3) 数据层集成

对于当代电子商务而言，商务数据的交换是应用的关键环节，随着在电子商务应用中(例如，B2B、B2C 应用，尤其是 B2B)商务信息交换的应用模式不断为主流应用开发所接受，面向通用领域的数据集成数据交换应用也成为了一个重要的 XML 应用领域，在这方面，不少电子商务应用领域(尤其是 B2B 应用)的解决方案在陆续进入这一更为泛化的领域。

(4) 应用层集成

当 XML 在经历了电子商务应用的经验之后，人们不仅逐渐地在数据层上完成应用系统(尤其是商务系统)的连接，同时在业务层或者函数层上希望能完成系统的互联，这也就是常说的 Internet 环境应用的广泛互联，这方面的技术主要是以 XML 为技术基础的 Web Services 系列技术。

(5) 系统配置信息描述

随着 XML 在各种各样应用开放中的延伸，原先系统软件、应用软件中使用文本文件、Profile 文件或者 INI 文件形式进行系统、应用配置信息管理的方式逐渐被使用 XML 文档的管理方式所替代。

7.2.1.2 CORBA

CORBA 是 Common Object Request Broker Architecture(通用对象请求代理体系结构)的缩写。通常提到的 CORBA 一般有两层意思，一层意思是指对象管理组织(OMG)提出的分布式对象体系结构标准，另一层意思是按这种体系结构标准开发的中间件产品。

OMG(对象管理组)定义的 CORBA 是一种分布对象体系结构，它的主要功能是为客户提供对象请求代理服务。如图 7.4 所示，它有 4 个主要部分：对象请求代理(ORB)、对象服务(CORBA Services)、通用设施(CORBA Facilities)和应用程序对象。ORB 是一种中间件，负责在对象之间建立客户/服务器的关系；对象服务定义了为分布对象所提供的系统级的基本功能；通用设施定义了能够直接被应用对象所使用的功能；应用对象则指所有以 CORBA 为运行环境的应用。其中 ORB 是 CORBA 的核心，它定义了一种与语言和平台独立的对象总线，通过它，对象能够透明地向本地或远程对象发送请求或从它们那里接收应答。由 ORB 负责完成寻找和激活对象、请求应答消息的打包和传送，并处理并发和异常等工作。

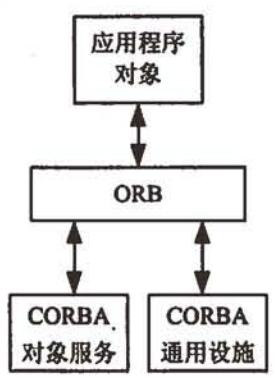


图 7.4　CORBA 体系结构

客户可以用动态或静态的方式通过 ORB 调用远程对象所公开的属性和方法。静态的调用方式是指在客户所采用的对象组件中明确定义了调用接口，客户程序可直接访问某远程对象的属性和方法；动态调用方式是指客户程序在构造和生成时并未确切规定远程调用对象，而是在运行时动态地确定所需访问的对象及其访问途径。在 CORBA 中，对象的接口由接口定义语言(IDL)描述，IDL 实现了对象接口描述与对象实现的分离。IDL 是一种独立于编程语言、下层网络和具体实现的数据类型描述语言，用于静态描述对象的接口。OMG IDL 描述指定了对象实现能够提供什么操作以及客户如何调用这些操作，因而也确定了系统对外提供的功能。

OMG IDL 语言仅提供了 ORB 系统所管理对象描述的概念框架，为了实现所描述的对象，必须将 IDL 映射到具体的编程语言，如 C，C++，Java 等。CORBA 规范中规定了 IDL 到具体编程语言的映射。一般的 CORBA 产品均包含一个称为 IDL 编译器的部件，该部件实现了 CORBA 规范中规定的 IDL 到某种特定编程语言的映射，将 IDL 描述编译成特定语言的头文件及客户方桩(stub)和对象实现方构架。在此基础上，开发者可以实现分布的客户和服务器系统。

具体来说，基于 CORBA 的分布式应用系统的开发过程如下：

(1) 用 OMG IDL 语言描述和定义接口。

(2) 用 IDL 编译器编译 IDL 描述文件，生成特定编程语言的头文件、客户方桩(stub)和服务器方构架。

(3) 实现服务器系统，包括使用特定的编程语言实现 IDL 文件中定义的接口，编制服务器方主程序，用于创建对象实例，完成初始化工作后，服务器处于等待接收请求状态，并通知系统。

(4) 服务器注册。

(5) 编制客户方主程序，用于连接服务器和使用服务器支持的对象。

CORBA 作为一种应用级的互联标准得到了广泛的认同和应用。其主要特征是：

- 在 CORBA 环境下应用系统间的互联是以对象或程序的调用方式进行的，这样就可以做到系统间实时互操作。这类环境有很强的互操作能力。原则上，一个系统内部能够完成的操作，在系统之间通过 CORBA 都可以实现。
- CORBA 的面向对象的特点还保证了各对象的封装性和内部细节的隐蔽性。这不仅可以简化各种功能的使用，还提高了系统的安全性。
- CORBA 比较适合于分层结构的应用集成，相对于当前广泛应用的多层结构系统设计来说，这一技术比较适合于核心业务逻辑的应用程序集成。此外，由于目前应用服务器大多提供 CORBA 接口，这样利用 CORBA 技术完成应用程序和平台之间的无缝连接也比较容易。

7.2.1.3 COM/DCOM 及 Windows DNA

分布式公共对象模型 DCOM(Distributed Component Object Model)是微软公司以其公共对象模型(COM)为基础提出的分布式应用集成框架，DCOM 和 Windows DNA(分布式因特网应用体系结构)是微软公司的组件集成标准，该标准支持基于数据总线和控制总线的组件集成。

COM 是一种技术标准，其商业品牌称为 ActiveX，它的特点是：组件遵循 COM 规范编写，是以 Win 32 动态链接库(DLLs)或可执行文件(EXEs)的形式发布的可执行二进制代码。遵循 COM 规范标准，组件与应用、组件与组件之间可以互操作，极其方便的建立可伸缩的应用系统。

COM 组件及其较高的可重用性展示了一种新的软件设计思路，以组件对象为中心的设计方法把硬件以芯片为中心的工艺思想恰如其分地融合于软件的面向对象的分析、设计和编写之中，使面向对象的概念和方法从工具语言的层次跃上了系统的应用层，也为 DNA 的思想奠定了物质基础。

Windows DNA(Distributed Internet Applications)是微软在 NT 平台上提出的分布式的互联网应用框架结构，被称为“数字神经系统”。这种结构的基本出发点是为了改善传统的 C/S 两层结构表现出的明显的局限性，以适应更快更复杂的事务处理任务和快速开发的需要。

Windows DNA 与微软的 Windows 操作系统紧密结合，是在原来微软的分布式对象服务(如 COM，交易服务器(MTS)等)的基础上构造的。Windows DNA 的结构和 SUN 的 J2EE 标准相似，如图 7.5 所示。

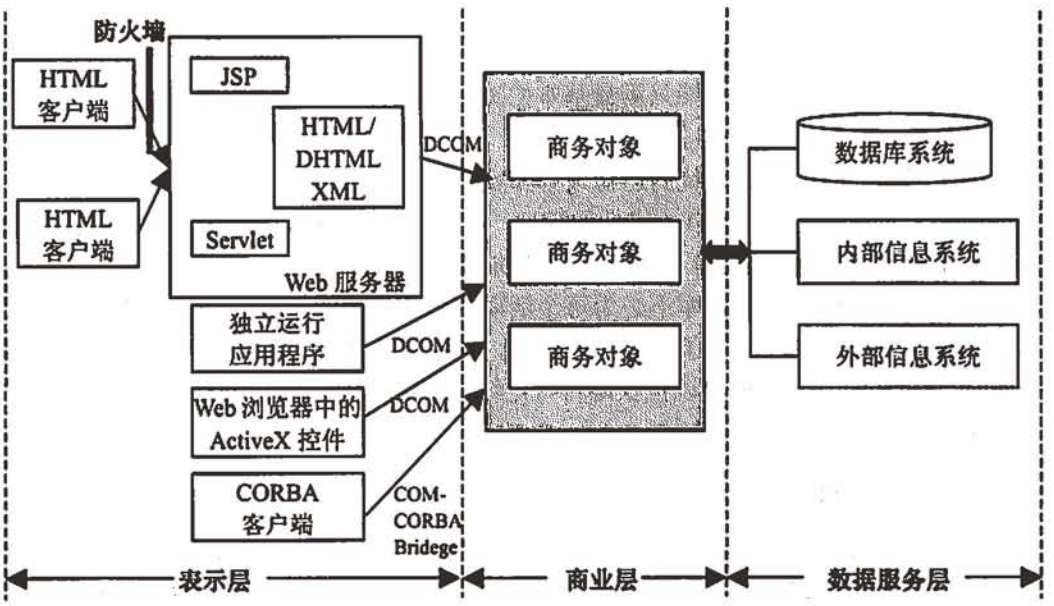


图 7.5　Windows DNA 结构图

在 Windows DNA 结构中，分布式应用系统由表示层、商业层和数据服务层三部分组成。

(1) 表示层：用户的界面部分。表示层包括 CORBA 客户端、Web 浏览器中运行的 ActiveX 控件、独立运行的应用程序、Internet 服务器 API(ISAPI)程序、活动服务器页面(ASP)和静态 Web 网页。客户端使用微软动态目录服务定位中间层组件，使用 DCOM 对其他组件进行方法调用。消息同样可以通过 MSMQ(微软报文队列)、COM+事件或其他组件技术进行异步发送。

(2) 商业层：商业层包括商业逻辑和数据逻辑，包含在 COM+组件中，负责处理表示层的应用请求，完成商务逻辑的计算任务，并将处理结果返回给用户。商业层是将原先置于客户端的商务逻辑分离出来，集中置于服务器部分，为所有用户共享。商业层是整个应用的核心部分，而组件对象模型(COM)则相当其心脏。商业层通过 COM 进行事务处理，并由 IIS(因特网信息服务系统)和 MTS(消息传递系统)为各种应用组件提供完善的管理。

(3) 数据服务层：为应用提供数据源。和以往的两层体系结构不同，数据库不再和每个活动客户程序保持一个连接，而是若干个客户程序通过应用逻辑组件共享数据库的链接，从而减少了连接次数，提高了数据服务的性能和安全性。可以根据需要选择 Microsoft SQL Server，Oracle 或任何与 OLE DB 或 ODBC 兼容的数据源。

Windows DNA 的技术思想使应用开发有了明确的分工。一部分人员专注于事务逻辑层 COM 组件的开发和测试工作，另一部分人员根据商务逻辑的需要选择和使用 COM 组件，而不需要了解组件功能实现的内部细节，最终以精练的 ASP 脚本语言把组件集成到页面之中，从而有效地降低了开发的难度。

将应用逻辑组件集中置于中间层，组件对象模型(COM)的可重用减少了应用系统整体的管理和维护费用。商务逻辑改变时，不必改变整个页面源代码，只需调整中间层相应的 COM 组件，即可灵活适应商务逻辑的变化。而后，系统可以在更新后的商务逻辑处理环境下运作，减轻了客户端应用程序版本控制和更新的难度。在这样的结构下，所有复杂的事务处理都在中间层进行，客户端只需最基本的浏览器配置，就可以和服务器及其他客户进行事务交流。

这种应用模式能够提高系统的运营效率和安全性。在中间层，IIS 负责应用逻辑层 Web 的管理，MTS 负责应用逻辑 COM 组件的管理。MTS 在多线程的支持下工作，实现对 COM 组件的分布式连接管理、线程自动管理及高性能事务处理的监视。应用程序使用组件可以共享与数据库的链接，使数据库不必为每个活动客户保持一个连接，而是若干个客户通过共享组件和数据库链接，降低了数据库的负担，提高了系统性。此外，客户通过组件访问数据库时，MTS 的安全管理可以按权限将特定组件授给不同的用户组，使商务活动的安全性和系统结构有机地结合在一起。

7.2.1.4 EJB 及 J2EE

EJB(Enterprise JavaBeans)技术是 Sun 公司所推出的 J2EE(Java2 Platform Enterprise Edition)中的核心技术之一，是 Sun 公司倡导的基于 Java 的组件构架。它是 Java 服务器端框架的技术规范(其最新规范是 2001 年 8 月发布的 Enterprise JavaBeans Specification, Version2.0)，定义了如何编写和部署服务器端组件，提供了组件与管理组件的应用服务器之间的标准约定。

EJB 体系结构定义了可重用、可移植的 Java 分布式事务服务器组件的设计和发布。它允许用 EJB 开发的应用程序在多个应用程序服务器上发布，不必为每个应用程序开发专门的服务器，当然这些服务器必须遵循 EJB 标准。EJB 使开发者可以把精力主要放在开发多用户的、高可靠性、高性能的应用程序上。通过使用和扩展 JDBC(Java 数据库连接性)，JNDI(Java 命名和目录接口)，RMI(远程例程调用)和 CORBA 等技术，EJB 标准提供了建立应用程序的统一方式，使这些程序具有永久性、事务处理、集群和负载均衡等能力，但又

不需要开发者直接实现这些能力。

在 EJB 之后，Sun 提出了 J2EE，定义了一个一致的环境，以支持企业级应用的集成，确保应用的可移植性。在 Sun 的 J2EE 规范当中，J2EE 被定义成为一个多层次的服务开发平台，总共包括以下 4 个组成部分，其核心是 J2EE 应用开发模型和 J2EE 平台。

- J2EE 规范　通过一整套详细的说明文档描述了 J2EE 架构，明晰了各角色之间的约束关系。
- J2EE 参考实现　是 J2EE 应用的标准宿主平台，包括一些 API 的和策略的集合。
- J2EE 兼容性测试工具　用来校验产品是否与 J2EE 平台相兼容。
- J2EE 应用编程模型　一个标准的开发多层架构服务的应用模型。

J2EE 应用编程模型如图 7.6 所示，在该模型中，商务逻辑处理被分成三个层次：客户层，中间层和企业信息系统层。

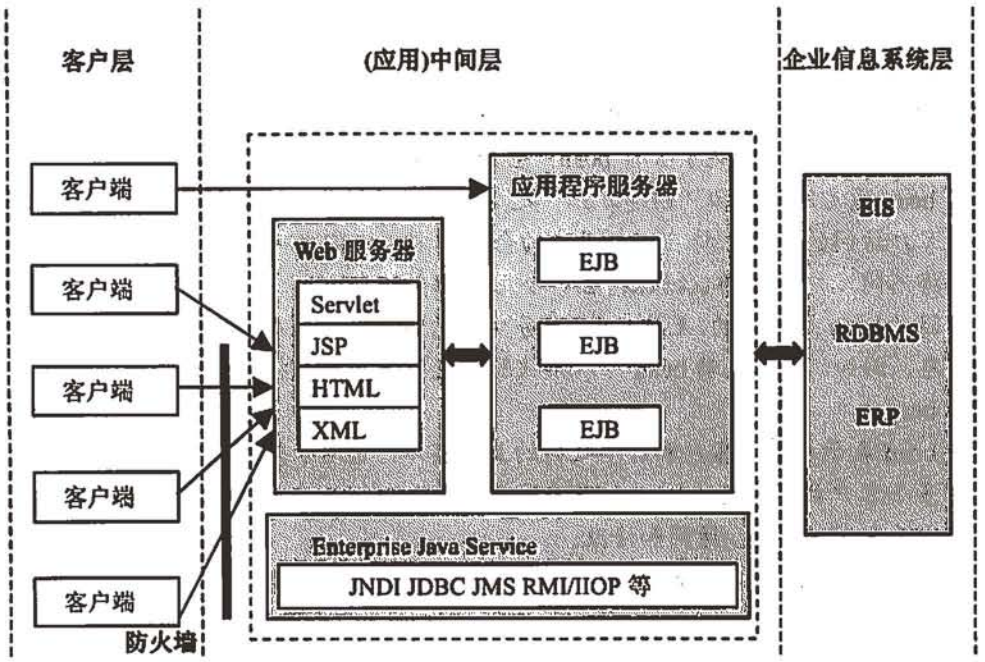


图 7.6　J2EE 应用编程模型

客户层支持不同的客户端，包括基于浏览器的瘦客户端及其他客户端，中间层能够完成企业服务的存取，企业信息系统层负责存储企业内部的关键商务数据。在 J2EE 模型中，应用服务被分为两部分，一部分是商务及逻辑，由开发人员实现；另一部分是标准的系统服务，由 J2EE 平台提供。

在 J2EE 应用编程模型中，中间层的商务功能通过一些 EJB 组件实现。中间层使用 JSP(Java 服务器网页)实现商务逻辑处理结果的动态发布，构成动态的 HTML 页面，中间层也可以使用 Servlet(小服务程序)实现更为灵活的一些动态页面。

中间层可以通过以下方式访问企业信息系统层中的信息资源：

- JDBC　数据库访问接口 API。
- Java 命名及目录接口(JNDI)　JNDI 可以获取命名服务和目录服务，例如 DNS，

NDS，LDAP 和 CORBA 的命名服务。

- Java 消息服务(JMS) JMS 作为一个标准的 API 接口可以和企业基于消息的中间件系统(例如 IBM MQSERIES，BEA TUXEDO 等)交互。
- Java mail Java mail 是基于 Java 的电子函件 API 接口。
- Java IDL IDL 是一种接口定义语言。Java IDL 可以通过建立远程接口支持 Java 和 CORBA 应用的通信。利用 Java IDL，应用系统可以调用 CORBA 的服务。

7.2.2 典型例题分析

例 1 简述 XML 的主要特点。

分析：详见 7.2.1.1 节。

答案：XML 的主要特点是自描述性、可扩展性、可校验性、层次结构、丰富的链接定义、多样的样式表支持。

例 2 EJB 2.0 规范定义了哪 3 种类型的 bean?

分析：EJB 2.0 规范定义了 3 种 bean: 会话 bean、消息驱动 bean 和实体 bean。

会话 bean 通常用来模拟“创建客户”之类的过程或任务。这些 bean 可以是有状态的，能使不同客户访问的数据保持在一个用户的会话期内。它们也可以是无状态的，在此情况下，不能将不同客户访问的数据保持在一个用户的会话期中。

消息驱动 bean 是异步的、无状态的、事务唤醒的组件，它可以处理由 Java 消息服务(JMS)发送的信息。例如，消息驱动 bean 可以接收股票交易消息，并将其发送给一个进行实际事务的会话 bean。

实体 bean 表示雇员、客户和订单之类的业务实体，它用来处理比较稳定的状态。实体 bean 可由多个客户共享。这类 bean 的状态通常与关系数据库中的各行相映射，关系数据库可以用其他的方式(如 SQL)访问和修改。

答案：会话 bean、消息驱动 bean、实体 bean。

7.2.3 同步练习

简述 CORBA 技术。

7.2.4 同步练习参考答案

公用对象请求代理程序体系结构(Common Object Request Broker Architecture)，缩写为 CORBA，是对象管理组织(Object Management Group)对应当今快速增长的软硬件的协同工作能力的要求而提出的方案。简而言之，CORBA 允许应用程序和其他的应用程序通信，而不论它们在什么地方或者由谁来设计。CORBA 1.1 由对象管理组织在 1991 年发布，定义了接口定义语言(IDL)和应用编程接口(API)，从而通过实现对象请求代理(ORB)来激活客户/服务器的交互。CORBA 2.0 于 1994 年的 12 月发布，定义了如何跨越不同的 ORB 提供者而进行通信。

ORB 是一个中间件，它在对象间建立客户与服务器的关系。通过 ORB，一个客户可以很简单地使用服务器对象的方法而不论服务器是在同一机器上还是通过一个网络访问。ORB 截获调用，然后负责找到一个对象实现这个请求，传递参数和方法，最后返回结果。客户不用知道对象在哪里，是什么语言实现的操作系统以及其他和对象接口无关的东西。

在传统的客户/服务器程序中，开发者使用他们自己设计的或者公认的标准定义设备之间的协议。协议的定义依赖于实现的语言，网络的传输和其他许多因素。ORB 将这个过程简单化。使用 ORB，协议定义是通过应用接口，而该接口是接口定义语言(IDL)的一个实现，它和使用的编程语言无关的。并且 ORB 提供了很大的灵活性。它让程序员选择最适当的操作系统，运行环境和设计语言来建设系统中每个组件。更重要的是，它允许集成已经存在的组件。

CORBA 是在面向对象标准化和互操作性道路上的一个信号。通过 CORBA，用户不必要知道软硬件的平台和它们处在企业网的什么地方就可以操作。

7.3　Web 服务

7.3.1　考点辅导

7.3.1.1　什么是 Web 服务

Web 服务是一段位于 Internet 上的业务逻辑，可以通过基于标准的 Internet 协议(诸如 HTTP 或 SMTP)访问。使用 Web 服务可能像登录到一个站点那么容易，也可能像解决一个多组织商业谈判问题那么复杂。

依照这个定义，近几年来采用的一些技术就应该被归为 Web 服务技术，但事实并非如此。这些技术包括 Win 32 技术、J2EE、CORBA 和 CGI(公共网关接口)脚本。这些技术和被称为 Web 服务的新技术之间的主要不同是它们的标准化，Web 服务新技术是在被全球大多数技术企业支持的 XML(与专用的二进制标准不同)的基础上的。XML 提供了一种与语言无关的方法来表示数据，而全球的厂商支持确保了每种主要新软件技术在近年内都会采用 Web 服务策略。

Web 服务具有以下特别的行为特征：

- 基于 XML　通过使用 XML 作为所有 Web 服务协议和新技术的数据表示层，这些技术就能够在核心层具备互操作能力。而在数据传送中，XML 消除了协议特有的网络、操作系统以及平台绑定限制。
- 松散耦合　Web 服务的用户不直接与 Web 服务关联，Web 服务接口能够随时变化，而不会降低客户和服务交互的能力。紧密耦合的系统是指客户和服务器在逻辑上紧密地相互结合，如果一个接口改变，另一个也必须更新。采用松散耦合体系结构使软件系统更加便于管理，并且使得不同系统间的集成更加容易。
- 粗粒度　面向对象的技术(诸如 Java)通过独立的方法指明其服务。独立的方法是过分细化的操作，以致于不能在一个共同的级别上提供有用的能力。从头开始创建一个 Java 程序需要创建几个细粒度的方法，然后将这些方法组合成由客户或者

其他服务使用的粗粒度服务。这些方法指明的业务功能和接口应该是粗粒度的。Web 服务技术提供了一种定义粗粒度服务的方法，这些服务可访问适量的业务逻辑。

- 同步或异步的能力　同步是指将客户绑定到服务的执行。在同步调用中，客户在继续执行前要阻塞并等待服务完成其操作。异步操作则允许客户激活服务然后运行其他功能。异步客户在稍后的时间点上获取其结果，而同步客户在服务结束的时候获取其结果。异步能力是启用松散耦合系统的一个关键因素。
- 支持远程过程调用(RPC)　Web服务允许客户使用基于XML的协议调用远程对象上的过程、函数和方法。远程过程暴露 Web 服务必须支持的输入和输出参数。近年来，运用 EJB(Enterprise JavaBeans)和 .NET 进行组件开发逐渐成为体系结构和企业部署的一部分。这两种技术通过一些 RPC 机制使软件成为分布式的和可访问的。Web 服务通过提供它自己的服务(这些服务和传统组件的服务等价)或者将传入的调用转化成对 EJB 或者.NET 组件的调用来支持 RPC。
- 支持文档交换　XML 的主要优点是它不仅仅是数据的通用表示方式，也是复杂文档的通用表示方式。这些文档可能很简单，比如在表示一个当前地址的时候；同时也可能是复杂的，比如在表示整个一本书的时候。Web 服务支持文件的透明交换，极大地方便了业务集成。

7.3.1.2 主要的 Web 服务技术

1. SOAP

(1) 背景

简单对象访问协议(Simple Object Access Protocal，SOAP)最初是由 Vserland Software 公司的 Dave Winter 创建的基于 XML 的 RPC 机制的想法。20 世纪 90 年代后期，此想法在 DevelopMentor 公司的 Winer，Don Box 和 Microsoft 的共同努力下，发展成了 SOAP 版本 0.9。其主要目的是为了使用 HTTP 协议来调用远程的 COM 对象，以跨越网络和防火墙的限制，提升 COM 的使用能力。随着 IBM 等公司的加入，SOAP 慢慢不再局限于 Windows 平台，被衍生到了 Java 平台，该协议也不再仅仅是基于 HTTP 协议，SMTP、FTP 也都可以绑定到 SOAP 上，SOAP 这种跨平台、跨语言、跨协议地完成对象互联的方法渐渐显露出了它的优越性。SOAP 可以看成是分布式对象访问技术的一个新的特性。

在主流的分布式对象技术中，无论是 CORBA 中的组件模型，还是 COM+中的 COM/DCOM，或是 J2EE 中的 EJB 都为分布式对象操作提供了一个很优秀的解决方案和技术架构。然而现代应用的需求绝不会希望解决方案被束缚在一个平台之中，一个企业所挑选的各种软件产品很可能会涉及到各种组件平台，这可能是因为时间的因素，也可能是因为部门的因素，当然更可能是因为竞争的因素，而 B2B 商务的全球化需要企业从内部到外部实现广泛的系统互联，从 EAI 到 B2B，异构系统、异构组件平台的互联是一个迫切需要解决的问题。

随着 SOAP 的出现，越来越发现这是解决不同组件平台互联的一个理想技术，此时，XML 已经得到广泛的应用，大多数平台已经有了能够使用的 XML 的处理器，使用 XML 重新描述和包装各自远程组件访问协议，以使得各种组件平台的远程访问协议都能通过同

一个标准的消息进行传输，这就是 SOAP 的初始概念。

(2) 组成

SOAP 由以下 4 个部分组成：

- SOAP envelop(SOAP 封套)　它构造定义了一个整体的表示框架，可用于表示在消息(message)中的是什么，谁应当处理它，以及这是可选的还是强制的(所谓可选的就是可以由目标应用程序自己选择是否处理，而强制的则是表明必须处理，如果无法处理，则需要返回错误)。
- SOAP encoding rules(SOAP 编码规则)　它定义了一个数据的编序机制，通过这样一个编序机制来定义应用程序中需要使用的数据类型，并可用于交换由这些应用程序定义的数据类型所衍生的实例。例如，可能应订单服务的需要，使用 SOAP 编码规则定义了订单的数据类型，并可以在订单生成的客户端与订单服务之间交换订单实例。
- SOAP RPC representation(SOAP RPC 表示)　它定义了一个用于表示远端过程的调用和响应的约定。
- SOAP binding(SOAP 绑定)　它定义了一个使用底层传输协议来完成在节点间交换 SOAP 封套的约定。

为了简化 SOAP 的复杂度，这 4 部分在功能上是正交的。特别的，封套和编码规则是被定义在不同的 XML 命名空间(namespace)中，这样有利于通过使用模块化的设计获得实现的简明性。

在 SOAP 规范中，还定义了两种 SOAP 绑定(binding)，用于描述 SOAP 消息(message)如何通过带 HTTP 扩展框架(HTTP Extension Framework)的 HTTP 消息(message)进行传输，或者是如何通过不带 HTTP 扩展框架的 HTTP 消息(message)进行传输。

(3) 概念

在 SOAP 规范中涉及以下一些重要的概念：

① 协议

- SOAP　它关于 SOAP 消息的格式和处理规则，是为沿着 SOAP 消息传输路径交换消息而需要的，是在不同应用程序之间生成和接收 SOAP 消息的交互过程的简单控制机制的一整套规范和约定。
- SOAP 绑定　它为传输的需要而将 SOAP 消息在另一个底层网络传输协议之上或之内传输的一整套规范和规则。典型的 SOAP 绑定包括在 HTTP 消息中传送 SOAP 消息等。
- SOAP 节点　它根据 SOAP 定义的整套规范来处理 SOAP 消息。SOAP 节点有责任遵守 SOAP 消息交换的规则以及提供通过依赖底层协议的 SOAP 绑定来访问的服务。任何不符合 SOAP 绑定的情况都将导致 SOAP 节点产生一个 SOAP Fault(SOAP 错误)。

② 数据封装

- SOAP 消息　它是在对等 SOAP 节点间通信的基本单位。
- SOAP 封套　它是 SOAP 规范中定义的 SOAP 消息(SOAP message)在句法上的最外层结构。在句法上，它包含了所有其他的 SOAP 元素和应用元素。

- SOAP 条目 它是一个句法上的结构，用于包含一个逻辑上需要被 SOAP 节点处理的单一元素，一个 SOAP 条目是由该条目最外层元素的完整修饰名(带命名空间修饰)所标识的，这个完整修饰名是由一个局部名和一个命名空间 URI(统一资源标识符)组成的。封装在 SOAP Header 中的 SOAP 条目称为 Header 条目，而封装在 SOAP Body 中的 SOAP 条目称为 Body 条目。
- SOAP Header 它是能够被 SOAP 消息传输路径中任意的 SOAP 接收者节点处理的一组 SOAP 条目(零个或多个)。
- SOAP Body 它是能够被 SOAP 消息路径中的最终 SOAP 接收节点处理的一组 SOAP 条目(零个或多个)。
- SOAP Fault 它是 SOAP 节点产生的用于包含错误消息的特殊的 SOAP 条目。
- SOAP 数据模型 它是一组抽象的构造约定，用于描述通用的数据类型和数据中的链接关系。
- SOAP 数据编码 它表示在 SOAP 消息中使用一个或多个 SOAP 条目，按照 SOAP 数据模型完成句法上的数据表示。

③ 消息接收和发送

- SOAP 发送者 它是发出 SOAP 消息的 SOAP 节点。
- SOAP 接收者 它是接收 SOAP 消息的 SOAP 节点。
- SOAP 消息路径 它是指为传送一个简单的 SOAP 消息而要经过的一组 SOAP 发送者和接收者。其中包含了初始 SOAP 发送者、零个或多个 SOAP 中介节点以及最终的 SOAP 接收者。
- 初始 SOAP 发送者 它是 SOAP 消息的最初产生者，同时也是 SOAP 消息路径的第一个节点。
- SOAP 中介节点 它既是 SOAP 接收者也是 SOAP 发送者，是 SOAP 消息可到达的某一个应用程序。当 SOAP 消息沿着 SOAP 消息路径传输时，SOAP 中介节点将处理一组确定的 SOAP 条目，然后它将消息转发给消息路径的下一个 SOAP 节点，直至传送到最终 SOAP 接收者。
- 最终 SOAP 接收者 它是指由初始 SOAP 发送者指定的通过 SOAP 消息路径传输的 SOAP 消息的最终的接收者。如果在 SOAP 消息路径中有 SOAP 节点产生了 SOAP 错误，那么 SOAP 消息将不会到达最终接收者。
- SOAP 应用 它是一个生产、消费 SOAP 消息或者对 SOAP 消息实施一些其他的动作的软件实体，在处理 SOAP 消息时，其行为是遵循 SOAP 处理模型的。

2. WSDL

SOAP 消息接收/发送格式的采纳带来了一种用同等结构化的方式来描述操作信息的需求。引入 WSDL 就是为了满足这种需求。

WSDL(Web Services Description Language，Web 服务描述语言)是一种将 Web 服务描述为一系列访问端点(endpoint)的 XML 文法，这些端点具有以面向过程或者面向文档的方式交换消息的能力。

在某种层次上，WSDL 与 CORBA IDL 或者 Microsoft IDL 并没有什么不同。它们都用于定义编程逻辑中对外敏感部分的接口和数据类型。

在另一种层次上，WSDL 又是完全不同的，它在一定程度上提供了 IDL 规范中缺乏的扩展能力。这些扩展使得 WSDL 可以用于：

- 描述端点和它们的消息，而不管消息格式或者用于交换消息的网络协议是什么。
- 将消息作为交换中数据的抽象描述。
- 将端口类型(port type)作为 Web 服务操作的抽象集合。于是，端口类型可以映射到具体的协议和数据格式。

随着 Internet 所采用的各种通信格式和协议的不断增多，找到一种描述两台机器间应该如何相互通信的标准方式已经变得越来越重要了。WSDL 描述一项服务做什么，如何调用它的操作以及在哪儿找到它。WSDL 已经建立了单独的定义和术语来定义 Web 服务、Web 服务存在的通信端点、Web 服务输入和输出消息的合法格式以及说明与具体协议和数据格式绑定的抽象方式。

在 WSDL 文件中定义的每样东西都是抽象的，它只是对参数和运行时应该如何通信的约束的定义。Web 服务实现必须符合 WSDL 文件中定义的指导方针，但是在此基础上也具有一些灵活性。WSDL 也提供了定义绑定的能力，将一系列抽象的消息定义与一种具体的协议或者数据格式相绑定。绑定扩展是一种为主要协议定义的绑定类型。WSDL 为 SOAP1.1、HTTP GET、HTTP POST 和 MIME(通用多功能因特网邮件扩充服务)定义了外部绑定扩展。

使用 WSDL 有如下几个好处：

- WSDL 提供了一个更为结构化的定义 Web 服务接口的方法，因而使得编写和维护服务容易了许多。
- WSDL 使得编写、调用 Web 服务所必需的客户端程序的代码量以及可能的错误量减少。
- WSDL 使实现改动更容易，减少了对 SOAP 客户端应用程序的不利影响。动态发现 WSDL 描述机制使得这些改动被自动地推到了使用 WSDL 的客户端，这样那些潜在的需要对客户端代码进行大修改的变动就不必每次都进行。

WSDL 当然并不是完美的。目前，还没有对 WSDL 描述版本控制的支持，因此 Web 服务提供者和客户必须认清当 WSDL 描述发生大的变化时，很可能问题就会被推到客户端一边。不过总的来说，对 WSDL 描述的态度应该与对传统的对象接口的态度相同——也就是一旦服务被定义并在实际应用中使用后，一般就不会再改变定义了。

3. UDDI

UDDI(Universal Description，Discovery and Integration，通用描述、发现和集成)规范提供了一个发布与发现 Web 服务的标准方法。UDDI 是由业界发起的规范，它试图创建一个与平台无关、开放的架构，用来描述、发现以及集成商业服务。UDDI 最关注的是面向服务的体系结构中“发现”服务的过程。

Web 服务正在逐渐成为所有形式的电子商务的基础。一个企业通过调用其他企业的服务去完成一个业务交易。在只有少数几个企业参与的情况下，人工管理这些业务伙伴的发现并不复杂。毕竟，判断仅有的几个业务伙伴中谁能提供你所需要的服务的过程并不复杂。然而，当业务伙伴越来越多，他们提供的接口的数量和种类也越来越多的时候，这种模型就不再适用了。怎样去发现所有可能和你进行交易的业务伙伴呢？如果试图手工地去查询，

那永远都不能确定是否已经发现了每一个可能的合作方。UDDI 是一个概念上的注册中心，它分布在多个节点中，这些节点彼此复制它们的业务数据。UDDI 服务注册中心(在 Internet 上由不同业务实体来管理)试图解决这个问题。

在 UDDI 之前，业界还没有什么通用的方法可以使业务实体直接通过产品和 Web 服务信息来和顾客以及业务伙伴联系。也没有一个统一的方法来说明如何集成业务伙伴之间已经存在的系统。没有什么东西尝试着通过一小段代码，在全球范围内从业务以及开发的角度发布和存储信息。

从概念上讲，一个业务实体可以在 UDDI 注册中心里注册白页、黄页、绿页三种类型的信息。UDDI 规范并没有直接声明这些类型，但是它们很好地总结了 UDDI 能够为业务实体存储哪些信息：

- 白页　基本的企业联系信息以及企业标识符，包括名称、地址、联系信息以及惟一的企业标识符。这些信息使得其他企业能够通过你的企业标识符来发现你提供的 Web 服务。
- 黄页　使用不同的分类法来描述 Web 服务的信息。这些信息使其他企业能够通过标准分类法来发现自己企业的 Web 服务。
- 绿页　企业所提供的 Web 服务的技术信息(服务的行为以及支持的功能)。这些信息包含了一些指针，指向 Web 服务分类信息和 Web 服务的存储地址。

UDDI 本质上是为解决当前在开发基于组件化的 Web 服务中所使用的技术方法无法解决的一些问题。UDDI 具有技术上的简单性，为 Web 服务在技术层次上提供了以下三个重要的支持：

- 标准化的、透明的、专门描述 Web 服务的机制。
- 调用 Web 服务的简单机制。
- 可访问的 Web 服务注册中心。

4. SOAP，WSDL 和 UDDI 之间的关系

图 7.7 可以说明 SOAP，WSDL 和 UDDI 三种技术之间的关系。

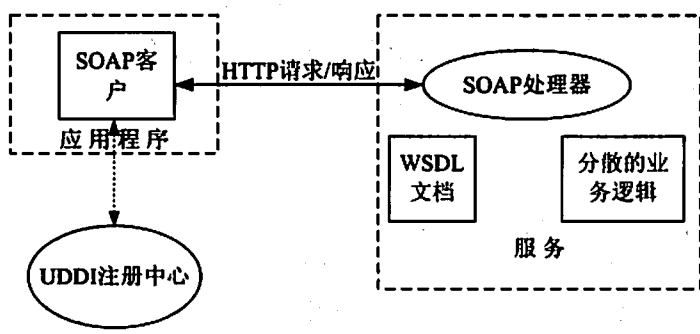


图 7.7　简单 Web 服务交互

SOAP，WSDL 和 UDDI 之间的关系可以描述如下：一个作为 Web 服务客户角色的应用程序，需要找出位于网络上某处的另一个应用程序或业务逻辑单元。客户通过名字、分类、标识符或者所支持的规范查询 UDDI 注册中心。一旦找到，客户便从 UDDI 注册中心获取 WSDL 文档的位置信息。WSDL 文档包含了关于如何联系 Web 服务的信息，以及 XML

模式中的请求消息格式。客户按照 WSDL 中发现的 XML 模式生成一个 SOAP 消息，并发送一个请求给主机(服务所处的位置)。

7.3.2　典型例题分析

例　列举 Web 服务的基本特征。

分析：详见 7.3.1.1 节。

答案：基于 XML、松散耦合、粗粒度、同步或异步的能力、支持远程过程调用(RPC)、支持文档交换。

7.3.3　同步练习

如何提高 Web 服务的安全性？

7.3.4　同步练习参考答案

可以从以下三方面入手提高 Web 的服务安全性：身份验证、保密性和完整性和可用性。

身份验证是指验证某人(或某物)是否与他们(它们)身份相符的过程。身份验证需要称为凭据的证据。最常见的凭据形式是密码。针对 Web 服务(以及多数 Web 应用程序)的最简单的身份验证形式是基本身份验证处理。

保密性和完整性是指确保在传输过程中所传输的信息不被盗窃或篡改的过程。这通常会涉及某种加密形式。针对 Web 服务(以及多数 Web 应用程序)最常见的加密形式是 SSL(安全套接字层)。

可用性是指确保信息在一段时间内是持久的，同时确保所需的功能对于请求它的任何人(或任何事物)而言都是可用的。由于 Web 服务可以由 Internet 上的任何人提供，因此，管理可用性意味着必须要处理 Web 服务不可用的情形。这主要涉及到固定性错误处理，也会涉及到调用队列。

7.4　本 章 小 结

本章主要要求考生掌握在网络应用中常见协议和规范的基本概念和内容，包括商用网络协议(SNA/APPN，IPX/SPX，AppleTalk，TCP/IP)、商务协议(XML，CORBA，COM/DCOM，EJB)和 Web 服务(WSDL，SOAP，UDDI)。

对本章的学习关键是要把握这些常见协议和规范之间的联系以及各自的功能和机制，抓住重点。每节中的习题将有助于理解和掌握大纲中的知识点。

第8章 网络设施

大纲要求：

- xDSL 调制解调器。
- ISDN 路由器接口、功能(非通信控制功能、NAT 功能)。
- 虚拟网(功能与机制)。
- FRAD(帧装配/拆除)、CLAD(信元装配/拆装)、接口，功能。
- 远程访问服务器的功能和机制。
- 办公室个人手持系统(PHS)。
- 中继式 HUB。
- L2，L3，L4 及多层交换机功能和机制。
- IP 路由器功能和控制。
- 与其他协议的共存(多协议路由器、IP 隧道)。

8.1 宽带网络接入方式

8.1.1 考点辅导

可以确信宽带是未来的趋势。随着宽带的发展，宽带的相关技术也成了热门的技术。本小节将介绍 xDSL 以及 ISDN 两种接入方式。

8.1.1.1 xDSL 调制解调器

DSL(Digital Subscriber Line)是数字用户线路，包括 HDSL(高速率数字用户线路)，SDSL(对称数字用户线路)，VDSL(甚高比特率数字用户线路)，ADSL(非对称数字用户线路)和 RADSL(速率自适应数据用户线路)等，一般统称为 xDSL。它们的主要区别体现在信号传输速度和距离的不同以及上行速率、下行速率对称性的不同。其中，ADSL 因其技术较为成熟，已经有了相关的标准，所以发展较快，也倍受关注。

ADSL 属于非对称式传输。它以铜质电话线作为传输介质，可在一对铜线上支持上行速率 640 Kb/s~1 Mb/s、下行速率 1 Mb/s~8 Mb/s 的非对称传输，有效传输距离在 3km～5km 范围内。

RADSL(Rate-Adaptive DSL，速率自适应 DSL)能够提供的速率范围与 ADSL 基本相同，但是它可以根据铜质电话线质量的优劣和传输距离的远近动态地调整用户的访问速度，使 RADSL 成为网上高速冲浪、视频点播(VOD)、访问远程局域网的理想技术，因为在这些应用中用户下载的信息往往比上传的信息(发送指令)要多。目前，我国深圳地区就是使用 RADSL。一般将 ADSL 和 RADSL 统称为 ADSL。

好比使用电话拨号接入一样，ADSL 需要使用 Modem 进行拨号，然后接入 Internet。

用户通过 DSL 访问 Internet，同样需要使用 DSL 调制解调器，我们称之为用户终端设备(CPE)。用户终端设备(CPE)是所有局域网到广域网通信的连接点。CPE 设备可以是一个在以太网和 ATM(异步传输模式)之间进行桥接的简单的调制解调器，也可以是一系列设备，其中每个设备都执行特定的功能，例如：地址转换、IP 路由器和桥接。很明显，利用多个分离的设备会增加网络的复杂性，同时安装、配置和维护设备的成本和工作量也会增加；所以当前的主流 DSL 调制解调器都将多种功能集成为一体。

ADSL 技术的特点表现如下：

- 直接利用用户现有电话线路，节省投资。
- 采用点对点的拓扑结构，用户可独享高带宽。
- 节省费用，上网、通话互不影响。
- 安装简单，只需要在普通电话线上加装 ADSL Modem，在电脑上装上网卡即可。

下面以 ADSL 作为例子，详细说明 ADSL 的工作流程：

(1) Internet 主机的数据经过传输链路传到电话公司的中心局。

(2) 在中心局，ADSL 访问多路复用器(Mutiplexer)调制，并将用户数据进行编码，然后整合来自普通电话线路的语音信号。

(3) 被整合后的语音和数据信号经过普通电话线传输到用户家中。

(4) 用户端的 ADSL Modem(也就是 ADSL 调制解调器)分离出数字信号和语音信号，数字信号经过解调和解码后传送到用户的计算机中；而语音信号则传送到电话机上，两者互不干扰。

8.1.1.2　ISDN 路由器

目前，基于模拟通信方式的公众电话网(PSTN)已不能满足人们对集成语音、数据、图像等综合业务的处理需要，因此我们面临着两种选择：一种是重新铺设高速线缆，新建一个网络；另一种是继续使用现成的公众电话网，但技术上要进行创新、改造。ISDN(Integrated Services Digital Network，综合业务数字网络)就是后者的实际技术方案。我国在 20 世纪 90 年代初建成了第一个 ISDN 网络，并且在 1996 年正式向用户提供 ISDN 业务，被称为“一线通”。

根据所提供带宽的不同，ISDN 可分为窄带(N-ISDN)和宽带(B-ISDN)两种。目前，与 N-ISDN 相关的标准已非常完善，技术已经相当成熟，各类接入设备也很丰富，是 ISDN 的主要应用领域。国内电信机构曾经推出的“一线通”即为 N-ISDN 中的一种服务。而有关 B-ISDN 的技术相对较为复杂，主要是基于 ATM(异步传输模式)提供 150Mb/s 以上速度的业务，而且与之相关的技术和标准还需要进一步完善，是将来的发展方向。

1. ISDN 接口

ISDN 用户端的网络接口有两种类型：PRI 和 BRI。PRI(Primary Rate Interface，基群速率接口)的速率为 2Mb/s，类似于模拟网络的中继接口；可以为用户提供高速语音/传真/数据业务，如中大规模的商业企业应用等。BRI(Basic Rate Interface，基本速率接口)的速率为 144Kb/s，类似于模拟网络的用户接口。通常遇到的接入技术(如“一线通”)是 BRI 接口，为用户提供低速语音/传真/数据业务，如本地呼叫、小型家庭办公(SOHO)、中小规模的市场营销等。

BRI 由 3 个信道组成：两个承载信道(B1 和 B2)和一个 Delta 信道(D)。通常 BRI 用下列公式表示：2B+D，每一个 B 信道是一个 64 Kb/s 全复用信道，用于用户各种类型的业务、语音、传真、数据、视频。另一方面，D 信道用于包交换数据业务和带外信令，其带宽对 BRI 为 16 Kb/s，对 PRI 为 64 Kb/s。每一个 2B+D BRI 数据线能同时处理三个以上的呼叫，其中两个可以是语音或者传真，第三个可以是包交换数据业务。对于 BRI 的网络接口，可以由两个 64Kb/s 的 B 信道(B1 和 B2)组成一个 128Kb/s 的数据管道。

PRI 支持的容量比 BRI 高，为商业用户提供 PBX(专用小交换机)功能或者局域网支持，因为在北美和欧洲使用不同的数字速率，所以，不可能在一个数据速率上达成一致。美国、加拿大、日本使用基于 1.544 Mb/s 的传输结构，即 T-1；而欧洲基于 E-1，传输速率为 2.048 Mb/s。基于 1.544 Mb/s(T-1)的传输结构，速率为 23B+D(23 个 B 信道加上一个 64 Kb/s D 信道)；基于 2.048 Mb/s(E-1)的传输结构，速率为 30B+D(30 个 B 信道加上一个 64 Kb/s D 信道)。和 BRI 类似，PRI 使用灵活，用公式可表示为：nB+D，用户可以根据需要请求一定数量的 B 信道。

ISDN 基于现有的公众电话网，通信线路就是普通的电话线，使用方法与使用普通电话时没有区别。但与普通模拟电话不同的是：ISDN 在线路上传输的是数字信号，而不是被处理之后的模拟信号。

2. ISDN 功能

为了定义 ISDN 用户—网络接口的配置，并建立相应的接口标准，CCITT 采用了功能群和参考点的概念：功能群(Functional Group)是用户接入 ISDN 所需的一组功能，这些功能可以由一个或多个设备来完成；参考点(Reference Point)是用来分割功能群的概念上的点。

在不同的实现方案中，一个参考点可以对应，也可以不对应于一个物理接口。应该注意的是，功能群和参考点都是抽象的概念，它们可能映射实际的物理结构，但又不同于物理的设备和接口。

(1) 非通信控制功能

根据功能群和参考点的概念，CCITT I.411 建议提出了 ISDN 用户网络接口的参考配置(如图 8.1)。

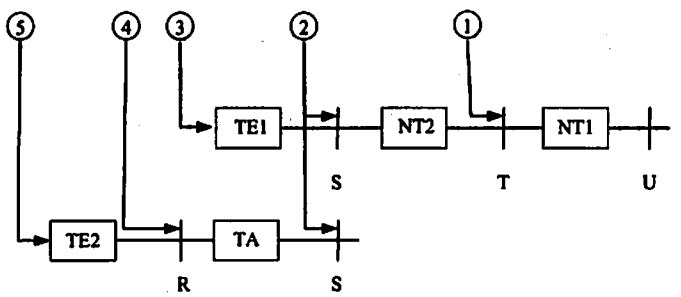


图 8.1 ISDN 网络接口参考图

如图 8.1，NT1 与 NT2 之间的参考点 T 是用户与网络的分界点，T 点右侧的设备归网管部门所有，左侧的设备归用户所有。参考点 S 对应于单个 ISDN 终端入网的接口，它将用户终端设备和与网络有关的通信功能分开。参考点 R 提供 ISDN 标准终端的入网接口，位于 TE2 和 TA 之间。参考点 U 对应于用户线，这个接口用来描述用户线上的双向数据信

号。但是，到目前为止，CCITT 还没有建立 U 接口的标准。

我们可再次归类：图 8.1 中的 1 和 2 点(即参考点 T 和 S)是承载业务的接入点。接入点 4(即参考点 R)使不符合 ISDN 标准的设备能够经过终端适配器(TA)的转换之后接到 ISDN 的承载业务接入点。3 和 5 点是用户终端业务的接入点；使用 ISDN 标准终端的用户终端业务从 3 点接入；使用非 ISDN 标准终端的用户终端业务从 5 点接入。下面是各功能群功能的详细描述。

① 网络终端 1(NT1，Network Termination 1)

NT1 包含 OSI 第一层的功能，即用户线传输终端的有关功能。NT1 是 ISDN 网在用户端的物理和电气终端装置。NT1 可能属于运行管理部门所有，是网络的边界。这个边界使用户设备不受用户线上传输方式的影响。NT1 负责线路的维护，例如：环路测试和性能监视等。NT1 还支持多个信道(如 2B+D)的传输，这些信道的信息在第一层上，用同步时分复用方法复用成统一的数字比特流。最后，NT1 还以点对点的方式支持多个终端设备同时接入。这时，NT1 具有解决 D 信道竞争的能力。

② 网络终端 2(NT2，Network Termination 2)

NT2 又叫做智能的网络终端。它可以包含 OSI 1~3 层的功能。NT2 可以完成交换和集中的功能。NT2 的例子有数字 PBX、集中器和局域网。数字 PBX 和局域网可以将一定数量的终端设备连接成局部地区的专用网络，提供本地交换功能，并经过 T 参考点和 NT1 将局部网络和 ISDN 沟通。集中器不能进行本地交换，但是它将一群本地终端的通信业务量集中起来，再和 ISDN 相连，以提高用户—网络接口上信道的利用率。

③ 1 类终端设备(TE1，Terminal Equipment Type 1)

TE1 又叫做 ISDN 标准终端设备。它是符合 ISDN 接口标准(S 参考点上的标准)的用户设备，例如数字电话机和 4 类传真机。TE1 完成用户端 1~3 层的功能以及面向某种应用的高层功能。

④ 终端适配器(TA，Terminal Adaptor)

TA 完成适配功能(包括速率适配及协议转换)，使 TE2 能接入 ISDN 的标准接口。TA 具有 OSI 第一层的功能以及高层功能。

⑤ 2 类终端设备(TE2，Terminal Equipment Type 2)

TE2 又叫做非 ISDN 标准终端设备，是不符合 ISDN 接口标准的用户设备。它包含了现有通信网中的终端设备，例如，具有 RS-232 物理接口的终端和具有 X.25 接口的终端，也可以是其他任何非标准设备。TE2 需要经过终端适配器 TA 的转换，才能接入 ISDN 的标准接口(S 参考点)。TE2 完成面向某种应用的高层功能以及和非标准接口(R 参考点上的标准)有关的低层功能。

(2) NAT 功能

另外，Intranet(企业内部网)通过 ISDN 接入之后，就可以通过 Internet 来发布信息，或进行信息检索。但是，随着 Internet 迅速发展，公网 IP 地址短缺已成为一个十分突出的问题。为了解决这一问题，出现了多种解决方案。使用 ISDN 路由器带有的 NAT(Network Address Translation，网络地址转换法)服务是其中一种解决方案。这样也是 ISDN 路由器特色功能的体现。

NAT 的功能是指将使用私有地址的网络与公用网络 Internet 相连，使用私有地址的内

部网络通过 NAT 路由器发送数据时，私有地址将被转化为合法注册的公共 IP 地址；从而可以与 Internet 上的其他主机进行通信。

NAT 路由器被置于内部网和 Internet 的边界上，并且在把数据包发送到外部网络前将数据包的源地址转换为合法的公共 IP 地址。当多个内部主机共享一个合法公共 IP 地址时，地址转换是通过端口多路复用(PAT)，即改变发出数据包的源端口并进行端口映射完成。

以下将详细描述 NAT 的工作流程。假设 ISDN 拨号之后，从 ISP 处获得的合法地址为 61.155.68.1/30；而公司内部网络地址为 192.168.0.0/24，路由器内部网络接口的地址为 192.168.0.254/24，广域网地址为 61.155.68.1/30。

如果 IP 地址为 192.168.0.1/24 的内部计算机向 Internet 上的服务器 202.119.9.112 发出请求，则 NAT 相应的操作过程如下：

① 内部主机 192.168.0.1/24 的用户发出到 Internet 上主机 202.119.9.112 的连接请求。

② 边界(ISDN)路由器从内部主机接收到第一个数据包时会检查其 NAT 映射表，如果还没有为该地址建立地址转换映射，路由器便决定为该地址进行地址转换。路由器为该内部地址 192.168.0.1 到合法 IP 地址 202.119.9.112 的映射，同时附加端口信息，以区别与内部其他主机的映射。

③ 边界(ISDN)路由器用合法 IP 地址 61.155.68.1 及某端口号来替换内部 IP 地址 192.168.0.1 和对应的端口号，并转发该数据包。

④ Internet 服务器 202.119.9.112 接到该数据包，并以该数据包的地址(61.155.68.1)来对内部主机 192.168.0.1 作出应答。

⑤ 当边界(ISDN)路由器接受到目的地址为 61.155.68.1 的数据包时，将使用该 IP 地址、端口号从 NAT 的映射表中查找出对应的内部地址和端口号，然后将数据包的目的地址转化为内部地址 192.168.0.1，并将数据包发送到该主机。对于每一个请求都重复第②~第⑤步。

8.1.2 典型例题分析

例 1 阅读以下说明，回答问题 1~问题 4。(2004 年上半年下午试题二)

【说明】

某小公司网络，如图 8.2 所示，其中路由器具有 ISDN 模块，公司网络通过 ISDN 连接到 ISP。

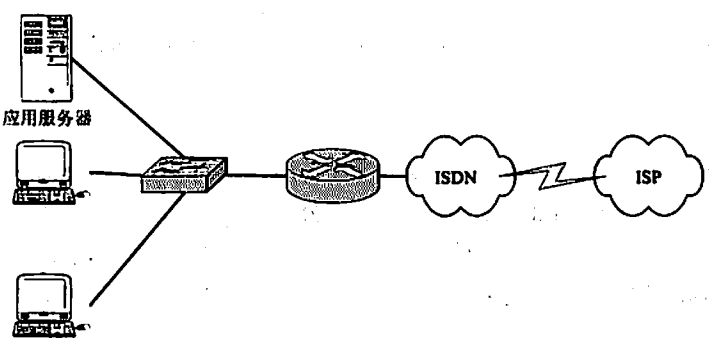


图 8.2 公司网络拓扑图

【问题】

1. 在应用服务器关机的情况下，公司员工能连接上 Internet 吗？简要解释。

2. 路由器与 ISDN 之间需要加入终端适配器(TA)吗？试说明在什么情况下要加入 TA。

3. 公司内电话、传真机与 ISDN 的连接情况如图 8.3 所示。请将图中(1)、(2)的空缺处的设备名称填写在答题纸的相应位置。

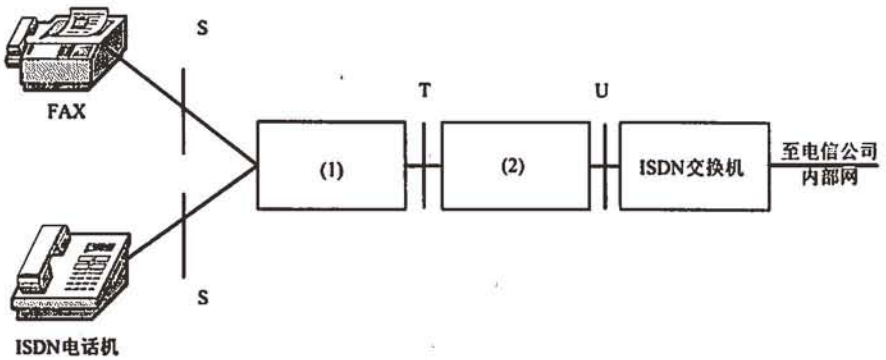


图 8.3　ISDN 接入网络

4. 假设采用 ISDN 基本速率接口，下载 1875K 的文件，最快要多少秒？

分析：公司内部网的主机都是通过 HUB(或者交换机)连到 ISDN 路由器的。而 ISDN 路由器拨号接入 ISP，然后通过 NAT 的功能将局域网的私有 IP 转换成合法的公共 IP，才能正常访问 Internet。整个过程都与应用服务器没有关系，因此，在应用服务器关机的情况下，员工仍能上 Internet。

TA(终端适配器)完成适配功能(包括速率适配及协议转换)，使 TE2(非 ISDN 标准终端设备)能接入 ISDN 的标准接口。因此，路由器与 ISDN 之间不需要加入 TA。

从图 8.1 中，我们得知，NT2(网络终端 2)是介于参考点 S 与 T 之间的网络设备，其例子有数字 PBX、集中器等。而 NT1(网络终端 1)是介于参考点 T 与 U 之间的网络设备。

ISDN 基本速率接口最高的速度可以达到：64Kb/s × 2 = 128Kb/s，即使用了两个 B 信道。而一个字节由 8 个比特位构成，因此需要的时间为：1875 × 1024 × 8/128000=120 秒。

答案：1. 可以正常访问 Internet。2. 不需要加 TA。3.(1)NT2；(2)NT1；4. 120 秒。

例 2　阅读以下说明，回答问题 1~问题 6。(2004 年下半年下午试题二)

【说明】

ADSL 是接入 Internet 的一种宽带技术，图 8.4 为一台带网卡的 PC 机采用 ADSL 接入 Internet 的网络结构图。

【问题】

1. 填写图 8.4 中(1)和(2)空缺名称。

2. ADSL 有哪两种 IP 地址的分配方式？

3. 目前在使用 ADSL 访问 Internet 时，要不要收取电话费？

4. 在本质上，ADSL 采用的是什么多路复用方式？

5. 使 ADSL 的传输速率更高有哪两个主要因素?
6. 按照 G.Lite 的最高速率标准，上传 24MB 的文件需要多少秒?

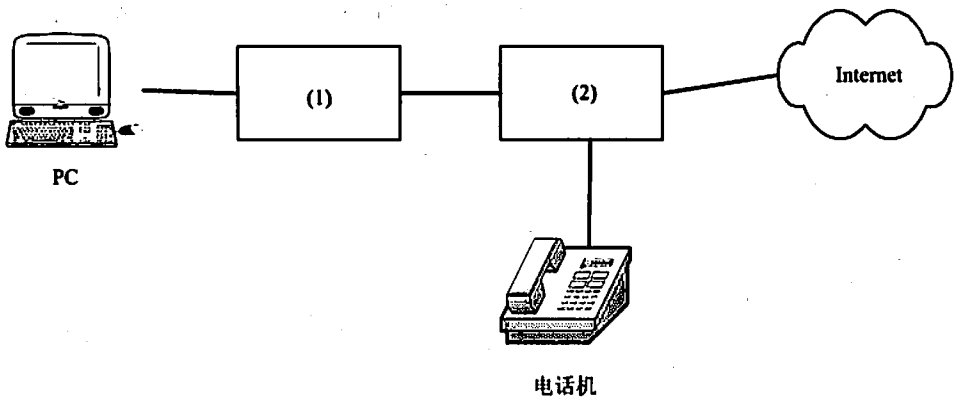


图 8.4 ADSL 接入网络拓扑图

分析: ADSL 技术是一种不对称数字用户线实现宽带接入互联网的技术，采用 FDM(频分复用技术)。ADSL 作为一种传输层的技术，充分利用现有的铜线资源，在一对双绞线上提供上行 640Kb/s、下行 8Mb/s 的带宽，从而克服了传统用户在“最后一公里”的瓶颈，实现了真正意义上的宽带接入。传统的电话系统使用的是铜线的低频部分(4KHz 以下频段)。而 ADSL 采用 DMT(离散多音频)技术，将原先电话线路 0Hz~1.1MHz 频段划分成 256 个频宽为 4.3KHz 的子频带。其中，4KHz 以下频段仍用于传送 POTS(传统电话业务)，20KHz~138KHz 的频段用来传送上行信号，138KHz~1.1MHz 的频段用来传送下行信号。DMT 技术可以根据线路的情况调整在每个信道上所调制的比特数，以便更充分地利用线路。一般来说，子信道的信噪比越大，在该信道上调制的比特数越多。如果某个子信道的信噪比很差，则弃之不用。

目前，ADSL 可达到上行 640Kb/s、下行 8Mb/s 的数据传输率。ADSL 充分利用了线路中没在用于语音呼叫的带宽部分。实质上，它把 1MHz 的带宽分成了 3 个信息通道：一个高速下行通道，一个中速双工(上行/下行)通道和一个常规的语音通道(下行是指数据从电话网传到用户端；上行则指的是数据从用户端发送到电话网络)。大多数 Internet 应用程序在上行和下行带宽上的需求并不相等。换句话说，用户在某个方向上传输的数据量比在另一个方向上传输的数据量更大。一般来说，Internet 用户访问、接收的信息比他们上传的数据多得多。这就是 Internet 的天性。用户阅读的电子邮件比他们发送的电子邮件多；下载的视频也比上传的视频量大。一个普通用户的上行能力通常也就局限于发送命令或传输小数据文件到服务器。总之，信息多属于下行数据。

在设计 ADSL 的时候就充分利用了这种不平衡的带宽趋势。从网络到订户(下行)的传输速率超过 8Mb/s，而从订户到网络(上行)的速率最高可以达到 640Kb/s。现在比较成熟的 ADSL 标准有两种，即 G.DMT 和 G.Lite，G.DMT 是全速率的 ADSL 标准，支持 8Mb/s 及 1.5Mb/s 的下行及上行速率，但要求用户安装 POTS 分离器，比较复杂且价格贵；而 G.Lite 标准速率低，下行速率为 1.5Mb/s，上行速率为 512Kb/s，但它不需要安装复杂的 POTS 分离器，适合于普通家庭用户。

ADSL Modem 采用 FDM 技术(Frequency Division Multiplexing，频分多路复用)和回波抵消技术(Echo Cancellation)两种技术划分可利用电话线路的带宽。

FDM 技术将频带划分为上行部分和下行部分，下行通道再被时分多路复用(Time Division Multiplexing)为一个或多个高速信道和低速信道；而上行通道也会被复用为相应的低速信道。回波抵消技术(Echo Cancellation)使上行通道和下行通道在频带上的重叠部分相互抵消，通过本地的回波抵消技术可以有效地分开上、下行信道，减小串音对信道的影响，从而实现信号的高速传送。

答案：

1. (1)ADSL Modem；(2)滤波器或 POTS 分隔器。
2. 静态(固定)和动态获得 IP。
3. 在中国地区，一般不需要收取电话费，但是需要收取数据通信费。
4. 频分多路复用。
5. 下行频段的低端与上行频段重叠、回波抵消技术。
6. G.Lite 的最高速率标准是下行 1.5Mb/s，上行 512Kb/s。则上传 24MB 文件需要的时间为：24×1024×8/512＝384 秒。

8.1.3　同步练习

1. 非对称数字用户线 ADSL 是采用__(1)__调制通过双绞线向用户提供宽带业务、交互式数据业务和普通电话服务的接入技术，其上行速率为 640Kb/s~1Mb/s，下行速率为 1Mb/s~__(2)__，有效传输距离为 3km~5km。ADSL 接入互联网的两种方式是：__(3)__。Cable Modem 又叫线缆调制解调器，可以连接用户家中的 PC 机和__(4)__网络。Cable Modem 的最高上行速率可达__(5)__，下行速率则更高，彻底解决了由于声音/图像传输而引起的阻塞。

2. N-ISDN 是在__(1)__基础上建立起来的网络，能够提供的最高速率是__(2)__。网络提供基本接口速率时，传输声音需要使用__(3)__，一路语音占用的数据传输率是__(4)__，占用户可用带宽的比例是__(5)__。

3. ADSL 有哪两种 IP 地址的分配方式？其采用哪一种多路复用方式？

4. 用户使用 ADSL 进行上网，需要使用什么技术才能让数字信号和语言信号互不干扰？

8.1.4　同步练习参考答案

1. (1) FDM　(2) 8Mb/s　(3) 专线接入和虚拟拨号
   (4) HFC(混合光纤/同轴电缆)　(5) 10Mb/s
2. (1)电话网　(2)144Kb/s　(3)B 通路(信道)　(4)64Kb/s　(5)50%
3. 动态和静态 IP 地址分配；ADSL 采用了频分多路复用方式。
4. 要在用户的接入端，使用滤波器或者 POTS 分离器来分离出数字信号和语音信号。然后数字信号经过解调和解码后传送到用户的计算机中；而语音信号则传送到电话机上。

8.2 虚 拟 网

8.2.1 考点辅导

虚拟网，又叫虚拟局域网(Virtual Local Area Network，VLAN)，该技术已经逐渐被人们所接受。虚拟网技术的出现和局域网交换技术是分不开的。局域网交换技术使用户抛弃了传统的总线技术，并在一定范围内代替了人们早已熟知的共享型介质。

虚拟网为本地网提供了一种解决方案。虚拟网中仍然需要路由器，仍然存在着广播流量。不同的是，在我们将交换技术和虚拟网技术相结合后，网段中的用户可以很少，甚至可以只有一个用户(一台主机)；而广播域则能大到包含上千个用户。另外，如果使用得当，虚拟网中的工作站可以移动到新的物理位置而不需要重新配置任何参数。

8.2.1.1 虚拟网的功能

虚拟网是指在交换局域网的基础上，采用网络管理软件构建可跨越不同网段、不同网络的端到端的逻辑网络。一个虚拟网组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个网络设备，允许处于不同地理位置的网络用户加入到一个逻辑子网中。

虚拟网是建立在物理网络基础上的一种逻辑子网，因此建立虚拟网需要相应的支持虚拟网技术的网络设备。当网络中的不同虚拟网间进行相互通信时，需要路由的支持，这时就需要增加路由设备。要实现路由功能，既可采用路由器，也可采用三层交换机来完成。

在使用带宽、灵活性、性能等方面，虚拟网都显示出很大优势。在虚拟网中能够方便地进行用户的增加、删除、移动等操作，提高网络管理的效率。它具有以下功能特点：

1. 控制广播风暴

一个虚拟网就是一个逻辑广播域，通过对虚拟网的创建，隔离了广播，缩小了广播范围，可以控制广播风暴的产生。广播流量被限制在软定义的边界内，从而提高了网络的安全性。

2. 提高网络整体安全性

通过路由访问列表和 MAC(传输媒体访问控制)地址分配虚拟网划分原则，可以控制用户访问权限和逻辑网段大小，将不同用户群划分在不同虚拟网中，从而提高交换式网络的整体性能和安全性。此外，在相同虚拟网内的主机间传送的数据不会影响到其他虚拟网上的主机，因此减少了数据窃听的可能性，极大地增强了网络的安全性。

3. 网络管理简单、直观

对于交换式以太网，如果对某些用户重新进行网段分配，需要网络管理员对网络系统的物理结构重新进行调整，甚至需要追加网络设备，从而增大网络管理的工作量。而对于采用虚拟网技术的网络来说，一个虚拟网可以根据部门职能、对象组成或者应用将不同地理位置的网络用户划分为一个逻辑网段。在不改动网络物理连接的情况下可以任意地将工作站在工作组或子网之间移动。利用虚拟网络技术，大大减轻了网络管理和维护工作的负担，降低了网络维护费用。在一个交换网络中，虚拟网提供了网段和机构的弹性组合机制。

8.2.1.2　虚拟网的机制

虚拟网是一种软技术，其如何分类，将决定此技术在网络中能否发挥到预期作用。下面将介绍虚拟网的分类以及特性。常见的虚拟网分类有 3 种：基于端口、基于 MAC 地址、基于网络层。

1. 基于端口

基于端口的虚拟网划分是比较流行的和最早的划分方式，其特点是将交换机按照端口进行分组，每一组定义为一个虚拟网。这些交换机端口分组可以在一台交换机上，也可以跨越几个交换机。

端口分组目前是定义虚拟网成员最常用的方法，而且配置也相当直截了当。纯粹用端口分组来定义虚拟网，不容许多个虚拟网包含同一个实际交换机端口。但是，用端口定义虚拟网的主要局限是：使用不够灵活，当用户从一个端口移动到另一个端口时，网络管理员必须重新配置虚拟网成员。

2. 基于 MAC 地址

基于硬件 MAC 地址定义的虚拟网既有优点又有缺点。由于数据链路层的 MAC 地址是硬连接到工作站的网络界面卡(NIC)上的，所以基于 MAC 地址的虚拟网使网络管理者能够把网络上的工作站移动到不同的实际位置，而且可以让这台工作站自动地保持它原有的虚拟网成员资格。按照这种方式，由硬件 MAC 地址定义的虚拟网可以被视为基于用户的虚拟网。

在这种方式的虚拟网中，交换机对终端的 MAC 地址和交换机端口进行跟踪。在新终端入网时，根据已经定义的虚拟网——MAC 对应表将其划归某一个虚拟网。无论该终端在网络中怎样移动，由于其 MAC 地址保持不变，故不需进行虚拟网的重新配置。这种划分方式减少了网络管理员的日常维护工作量，不足之处在于所有的终端必须被明确地分配在一个具体的虚拟网，任何时候增加终端或者更换网卡，都要对虚拟网数据库调整，以实现对该终端的动态跟踪。

基于 MAC 地址的虚拟网解决方案的缺点之一是要求所有的用户必须初始配置在至少一个虚拟网中。在初始手工配置之后，用户的自动跟踪才有可能实现。然而，这种不得不在一开始就先用人工配置虚拟网的方法的缺点在一个非常大的网络中变得非常明显：几千个用户必须逐个地分配到各自特定的虚拟网中。

3. 基于网络层

基于网络层的虚拟网划分也叫做基于策略(Policy)的划分，是这几种划分方式中最高级也是最为复杂的。基于网络层的虚拟网使用协议(如果网络中存在多协议的话)或网络层地址(如 TCP/IP 中的子网段地址)来确定网络成员。

4. VTP 与 STP

在虚拟网中应用最广的就是 VTP 和 STP 技术。VTP(VLAN Trunking Protocol)用于保持虚拟网配置统一性。VTP 在系统级管理虚拟网的增加、删除、调整时，自动地将信息向网络中其他的交换机广播。此外，VTP 减少了可能导致安全问题的配置。

VTP 的运行有 3 种模式：服务器模式、客户模式和透明模式。当交换机处在 VTP 服务

器模式或透明模式时，网管员能够在交换机上配置虚拟网。网管员通过使用 CLI、控制台菜单、MIB(使用 SNMP 简单网络管理协议管理工作站)修改虚拟网配置。

一个配置为 VTP 服务器模式的交换机向邻近的交换机广播虚拟网配置时，它通过 Trunk 端口，从邻近的交换机学习新的虚拟网配置。例如：当网络增加了一个虚拟网时，VTP 就将广播这个新的虚拟网，服务器和客户端的 Trunk 网络端口就准备接收虚拟网相关信息。

在交换机自动转到 VTP 的客户模式后，它会传送广播信息，并从广播中学习新的信息。但是，它不能通过 MIB(管理信息库)控制台菜单来增加、删除、修改虚拟网。VTP 客户端不能将虚拟网信息保存在非易失存储器(NVRAM)中。当设备启动时，它会通过 Trunk 网络端口接受广播信息，学习配置信息。

在 VTP 透明模式中，交换机不做广播或从网络学习虚拟网配置，可以通过控制台、CLI、MIB 来修改、增加和删除虚拟网。

为使虚拟网能够使用，必须使 VTP 知道其存在，并且虚拟网的相关信息要包含在 Trunk 端口的准许列表中。一个快速以太网 Trunk 端口自动为虚拟网传输数据，并且是从一个交换机传到另一个交换机。

而 STP(Spanning Tree Protocol)协议则能够提供路径冗余，并且可以使两台交换机中只有一条有效路径。

STP 协议在桥接(或交换)网络中定义了一棵树，并且迫使一定的备份路径处于备用状态。如果生成树中的网络一部分不可达，或者 STP 值变化了，生成树算法会重新计算生成树拓扑，并且通过启动备份路径来重新建立连接。STP 操作对于交换机来说是透明的，而不管交换机是连在 LAN 的某一部分还是多个部分。

当创建网络时，如果网络中所有节点都存在多条路径，则生成树中的算法可以计算出最佳路径。因为每个虚拟网是一个逻辑局域网部分，所以网管员可以使用 STP 工作在多个虚拟网中。

8.2.2 典型例题分析

例 阅读以下说明和交换机的配置信息，回答问题 1~问题 3。(2004 年上半年下午试题四)

【说明】

某公司下设三个部门，为了便于管理，每个部门组成一个虚拟网，公司的网络结构如图 8.5 所示。

交换机 Switch1 的部分配置信息：

```
Switch1(config)# interface f0/9
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 11
Switch1(config)# interface f0/10
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 12
Switch1(config)# interface f0/17
```

```
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 13
```

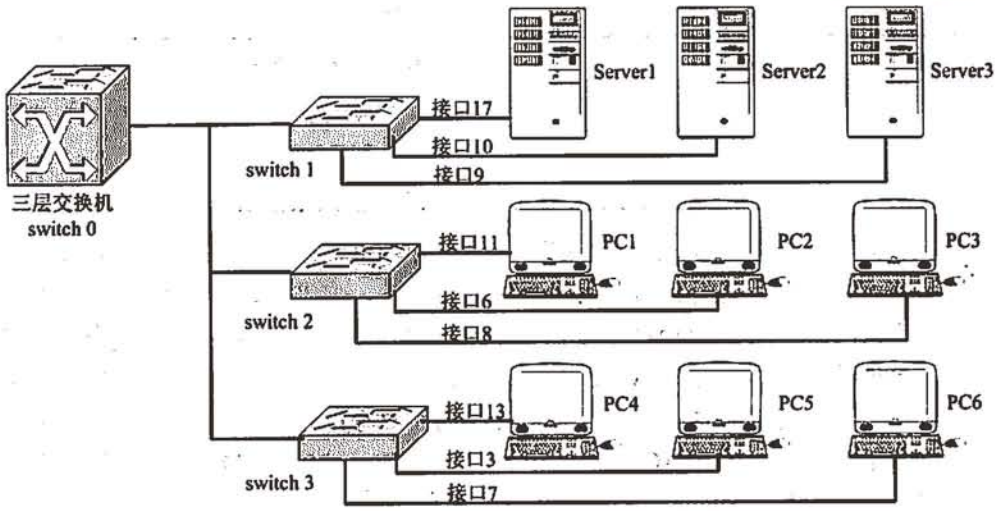


图 8.5　部门接入网络拓扑图

交换机 Switch2 的部分配置信息：

```
Switch2(config)# interface f0/6
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 11
Switch2(config)# interface f0/8
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 12
Switch2(config)# interface f0/11
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 13
```

交换机 Switch3 的部分配置信息：

```
Switch3(config)# interface f0/3
Switch3(config-if)#switchport mode access
Switch3(config-if)#switchport access vlan 11
Switch3(config)# interface f0/7
Switch3(config-if)#switchport mode access
Switch3(config-if)#switchport access vlan 12
Switch3(config)# interface f0/13
Switch3(config-if)#switchport mode access
Switch3(config-if)#switchport access vlan 13
```

【问题】

1. 通常虚拟网有静态和动态两种实现方式。这两种方式是怎么实现的，各有什么特点？Switch1 是使用哪种方式实现？

2. 在虚拟网中，STP 和 VTP 是什么协议？各有什么作用？

3. 填充虚拟网信息表(表 8.1)，将答案写在对应位置。

表 8.1 虚拟网信息表

部 门	虚拟网编号	包括的服务器和主机名
行政部	11	(1)
市场部	12	(2)
财务部	13	(3)

分析：在虚拟网的静态实现方式(也即是基于端口)中，网络管理员将交换机端口静态地分配给某一个虚拟网，这是经常使用的一种配置方式，容易实现和监视，比较安全。而在动态实现方式(也即使基于 MAC 地址)中，网络管理员必须先建立一个较复杂的数据库；然后，输入要连接的网络设备的 MAC 地址及相应的虚拟网号。这样，当网络设备接到交换机端口时，交换机自动把这个网络设备所连接的端口分配给相应的虚拟网。动态虚拟网的配置可以基于网络设备的 MAC 地址、IP 地址、应用的协议来实现。动态虚拟网一般通过管理软件来进行管理。Switch1 采用静态实现方式。

在虚拟网的实现机制中，STP(Spanning Tree Protocol)协议则能够提供路径冗余，并且可以使两台交换机中只有一条有效路径，防止环路的出现。STP 使用生成树算法，求解没有环路的最佳路径，使一些备用路径处于阻塞状态。大型交换网络中尤其是有多个虚拟网的时候，配置 STP 很重要。而 VTP(VLAN Trunk Protocol，VLAN 干道协议)用来管理虚拟网的删除、添加和修改等管理操作的一致性。在同一个 VTP 域内，VTP 通过干道端口在交换机之间传送 VTP 信息，从而使一个 VTP 域内的交换机能共享虚拟网信息。

从三台交换机的配置信息上，我们知道，这些端口都是采用静态的方式配置虚拟网的——将交换机的相关端口作为虚拟网的成员来完成虚拟网的访问。

答案：3.(1)Server3+PC2+PC5；(2)Server2+PC3+PC6；(3)Server1+PC1+PC4。

8.2.3 同步练习

1. IEEE 于 1999 年颁布了用以标准化虚拟网实现方案的__(1)__协议标准草案。虚拟网技术允许网络管理者将一个物理的局域网，__(2)__划分成不同的广播域(或称虚拟 LAN，即 VLAN)，每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。VLAN 是为解决以太网的__(3)__和__(4)__而提出的一种协议，它在以太网帧的基础上增加了__(5)__把用户划分为更小的工作组，限制不同工作组间的用户互访，每个工作组就是一个虚拟网。

2. 当 VLAN 跨越多个网段时，必须使用虚拟网独立路由器转发技术，试举例说明。

8.2.4 同步练习参考答案

1. (1) 802.1Q (2) 逻辑地 (3) 广播
   (4) 安全性 (5) 虚拟网头(或 VLAN ID)
2. 如图 8.6 所示。

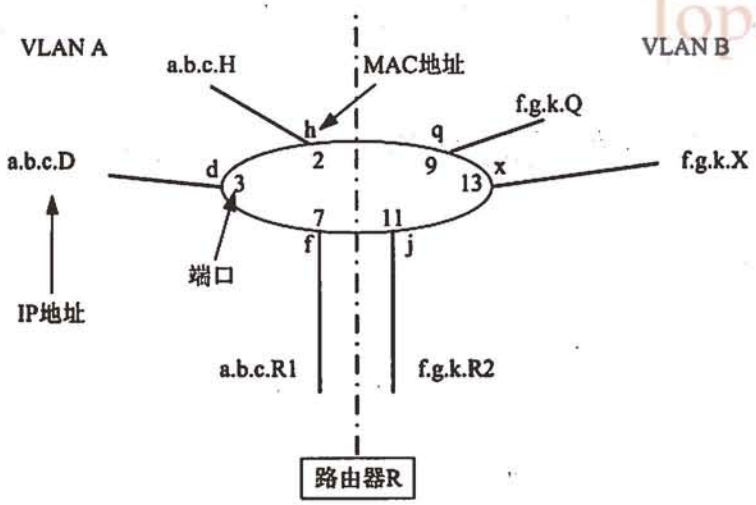


图 8.6　通过路由器连接 VLAN 示意图

假定有一个 16 端口的交换机，每 8 个端口连在一个独立的虚拟网上。每个站点都使用 IP 协议。端口 1~8 所连的站点使用同一个 IP 前缀(如图 8.6 所示，IP 前缀为 a.b.c)，其他 8 个端口上的站点使用另一个 IP 前缀(f.g.k)。该交换机桥接了端口 1~8；当这 8 个端口上的任何一个站点向该组内的其他站点发送包时，如果交换机还不知道目的地址(存储在 L2 的包头中)的位置，它将向这 8 个端口中的其他 7 个端口转发该包(发送该包的端口除外)。

如果包需要在局域网间进行交换，则需要通过路由器。一些交换机也可以在虚拟网间起到路由器的作用。假定交换机不能在虚拟网之间转发包，为了连接这些 VLAN，需要用一个路由器，每个 VLAN 连接到路由器的一个端口上。

图 8.6 中，左边的端口(2、3 和 7)位于虚拟网 A 中，右边的端口(9、11 和 13)位于虚拟网 B 中。路由器 R 连接到两个端口：虚拟局域网 A 中的 7 以及虚拟局域网 B 中的端口 11。

假定节点 H 希望发送一个包给节点 D。节点 H 的 IP 逻辑注意到 D 的 IP 前缀(a.b.c)与 H 的 IP 前缀相同，它们位于同一个局域网内。因此，H 将发出一个 ARP(地址转换协议)请求来找出 D 的数据链路地址(d)。现在 H 知道 IP 地址为 a.b.c.D 的节点的数据链路地址为 d，H 发送一个分组，其数据链路头部中，源=c，目的=d；IP 头部中，源=a.b.c.H，目的=a.b.c.d.D，与 D 进行通信。如果交换机还不知道数据链路地址 d 的位置，它将向虚拟网 A 中除端口 2 之外的其他所有端口转发这个包。如果交换机已经知道了 d 位于端口 3 上，则它只将该包转发给端口 3。

现在再假设节点 H 希望发送一个包给节点 Q。由于 Q 的 IP 前缀(f.g.k)不同于 H 的 IP 前缀(a.b.c)，H 的 IP 逻辑将通知 H 把这个包发给路由器。假定现在 H 已经知道了它所处的局域网上的路由器的 IP 地址为 a.b.c.R1。H 发出一个 ARP 请求来找出路由器的数据链路地址(本例中为 f)，然后发送一个包给 Q，该包中的数据链路头部的源=h，目的=f；IP 头部中，源=a.b.c.H，目的=a.b.c.d.Q。

路由器 R 接收该包，然后根据 IP 包头部的目的地址的 IP 前缀(f.g.k)判断它是属于 R 的右端口所连接的局域网。然后 R 发出一个 ARP 请求来找出 IP 节点(f.g.k.Q)的数据链路地址(q)。

现在路由器向虚拟网 B 转发这个包，其数据链路包头中，源=j，目的=q。IP 的头部跟原来一样，源=a.b.c.H，目的=f.g.k.Q。

8.3 FRAD(帧装配/拆除)、CLAD(信元装配/拆装)

8.3.1 考点辅导

当前，有两种高速分组技术可以构成宽带服务的基础：基于帧和基于信元的分组技术。FR(Frame Relay，帧中继)是由 X.25 发展起来的，加快了分组数据服务的传输技术，用于宽带数据服务。

而 ATM(Asynchronous Transfer Mode，异步传输模式)的设计目标则是：通过 ATM 网络为数据、语音、视频和任何其他 ATM 网络上的用户提供足够的服务。

8.3.1.1 FRAD 接口与功能

帧中继是在用户—网络接口之间提供用户信息流的双向传送，并保持信息顺序不变的一种承载业务。用户信息以帧为单位进行传输，并对用户信息流进行统计复用。帧中继也是综合业务数字网(ISDN)标准化过程中产生的一种重要技术，它是在数字光纤传输线路逐步替代原有的模拟线路，用户终端日益智能化的情况下，由 X.25 分组交换技术发展起来的一种传输技术。

帧中继完成了开放系统模型(OSI)物理层、链路层的功能；流量控制、纠错等功能改由智能终端去完成，这大大简化了节点机之间的协议，提高了线路带宽的利用率。帧中继主要应用在局域网(LAN)互联、高清晰度图像业务、宽带可视电话业务和 Internet 连接业务等。

但是，帧中继只定义了 UNI 和 NNI 的接口规程。因此，没有标准接口规程的局域网(LAN)要想接入到帧中继网络中，就需要通过 FRAD(Frame Relay Access Device，帧中继接入设备)将非标准的接口规程转换为标准的接口规程。FRAD 一般用于互联企业网络中的小型分支机构。FRAD 价格低，但是功能强，常常与 CSU/DSU(信道服务单元/数字务服单元)集成。FRAD 支持很多不同类型的传输业务，包括旧业务、LAN 和语音。支持各种旧协议的封装是从专用线路网络迁移到帧中继的关键；同时，FRAD 支持很多协议，是网络中很经济的接入点。FRAD 通常不执行传输介质之间的路由选择，也不像路由器那样提供丰富的安全功能。

8.3.1.2 CLAD 接口与功能

ATM 是一种信元中继技术。与 X.25 和帧中继不同，在这些系统中数据包和帧的长度是不固定的，但需在约定的范围内。所有 ATM 信元的长度都完全一样：53 个字节。在这 53 个字节中，5 个字节用于网络处理负荷，剩下的 48 个字节用于携带用户载荷。通过把数据单元尺寸固定在 53 个字节，ATM 具有可变长度数据单元所不具备的确定性，节点内部的缓存区管理也将得到很大的简化。

ATM 实现一般采用硬件方式，由经过特殊设计的高速芯片负责 ATM 协议的处理。使

用这种基于芯片的实现，使交换机中的队列时延从毫秒级下降到微秒级。因此，即使是在大型 ATM 网络上的实时传输业务，所累加的时延也很小。这种固定的 ATM 数据单元长度和以高速硬件实现的 ATM 协议相结合，使得 ATM 能够把所有传输业务类型汇聚到单一的非常经济的交换平台上。

ATM 是一种分层体系结构。ATM 分层由 OSI 参考模型的第一层(物理层)和第二层(数据链路层)构成。并且，ATM 本质上是一种数据链路实现。其数据链路层又可以分成上下两个层次：ATM 层(下半层)和 ATM 适配层(上半层)。

ATM 层的基本职责是以适当的方式在发送方和接收方之间交换信元；ATM 层上的基本数据单元是“信元”。至于 ATM 适配层(ATM Adaptation Layer，AAL)又可以进一步化分为两个子层。AAL 的较低子层是分段和重新装配(Segmentation And Reassembly，SAR)子层，AAL 较高子层是汇聚子层(Convergence Sublayer，CS)。ATM 适配层(AAL)的基本功能是将多种类型的传输业务汇聚或适配到 ATM 基础设施。因此，ATM 适配层(AAL)与具体传输业务类型有关。目前已经定义了四种 AAL。这四种 AAL 都使用相同的 SAR 子层，但是每种 AAL 类型实现自己与具体服务有关的 CS。

AAL SAR 子层主要负责接收从 CS 发送过来的任何信息，并构成 48 个字节的单元，作为 ATM 信元载荷。而 CS 负责接收来自上层(例如：IP 数据)的 PDU(协议数据单元)，并一般通过增加负荷进行适配。

在实际网络应用中，对于上行信道，来自各个 NT(网络终端)的用户数据(例如：IP 数据)由相应的 ATM 适配层(AAL)或 CLAD(信元装配/拆装设备)适配成 ATM 格式(信元化)，所形成的 ATM 信元进入到传输系统。而对于下行信道，则从传输系统接收到的 ATM 信元根据它们的 VPI/VCI 值进行分路，然后再转换成原数据送给用户。

8.3.1.3　ATM 的局域网应用(LANE)

ATM 作为广泛使用的主干网络，经常与局域网直接互联。此时，就需要使用 LANE 技术来减少互联所带来的相关问题。而 LANE 就是我们常说的仿真 LAN。LANE 规范对于将 ATM 与非 ATM 网络集成是非常关键的。LANE 定义了一个独立于协议的方法，采用这个方法，不同的 LAN 附属设备能够在一个 ATM 主干上进行通信。

LANE 在 OSI 模型的第二层进行操作，作为一个桥梁协议，使得定向连接的 ATM 网络与无连接以太网或令牌环类似。LANE 具有以下优点：

- 老式局域网装置，如 NIC(网络接口控制程序)以及它们与第二层相关的驱动软件，都与 LANE 兼容。
- 高层应用及上层协议能够在 LANE 上通信。
- 能够在 ATM 网络的任何地方找到一个 LANE 客户，包括在不同的地理位置，并且不被老式局域网的距离限制所束缚。
- 通常网络通信量拥塞不是问题，因为数据都是在独立的专用于仿真局域网的虚拟电路上传送的。

LANE 服务的另一个优点是不要求改变原有局域网中的任何硬件或软件。连接到以太网、令牌环或 FDDI(高速光纤环网)原有网络上的设备可以不做任何修改而加以使用，这意味着能够保护现有的网络投资。原有网络只要求一个局域网到 ATM 的接口，这是拓扑结构

和装置类型所要求的。

仿真局域网使用执行转换及管理过程的软件，这些软件驻留在 ATM 网络的不同设备中。两个主要的组件是局域网仿真客户(LEC)软件以及局域网仿真服务软件。LEC 软件可以应用在局域网到 ATM 的转换设备中或者作为驻留在 ATM 附属设备(如服务器的软件)的一部分。LEC 软件的主要功能是将 MAC 地址映射到 ATM 地址上，并进行地址解析。局域网仿真服务软件是在以下 3 个逻辑服务器上实现的：

- 局域网仿真服务器(LES) 它是在主服务器上的，提供地址注册以及 MAC 地址到 ATM 地址的解析，同时还有 ATM 地址路由说明符。
- 广播及未知服务器(BUS) 作为广播及多点传送控制中心，用于一个新站加入到仿真局域网时以及 ATM 信元到目的终端节点的位置查找及路由选择。
- 局域网仿真配置服务器(LECS) 包含有关 ATM 网络的所有配置信息，包括有关仿真局域网的所有信息。

这些服务器的实现必须事先就计划好，以便能够为 ATM 网络提供最好的性能和可靠性。所有这 3 个服务器都可以安装在一台 ATM 交换机上，或者分布在不同的交换机或是网络中与 ATM 兼容的路由器上。例如，LES 可以在一台 ATM 主干交换机上实现，LECS 可以运行在 ATM 附属服务器上，而 BUS 则可以驻留在一个局域网到 ATM 的接口模块上。

8.3.2 典型例题分析

例 1 阅读以下有关网络设计的叙述，分析网络结构，回答问题 1~问题 3。(2001 年下午试题三)

【说明】某企业从 20 世纪 50 年代中期开始使用 PC 机，历经 3+网络、Novell 网络的应用，后着手组建企业网络。经过需求分析和论证，设计出如图 8.7 所示的网络方案。

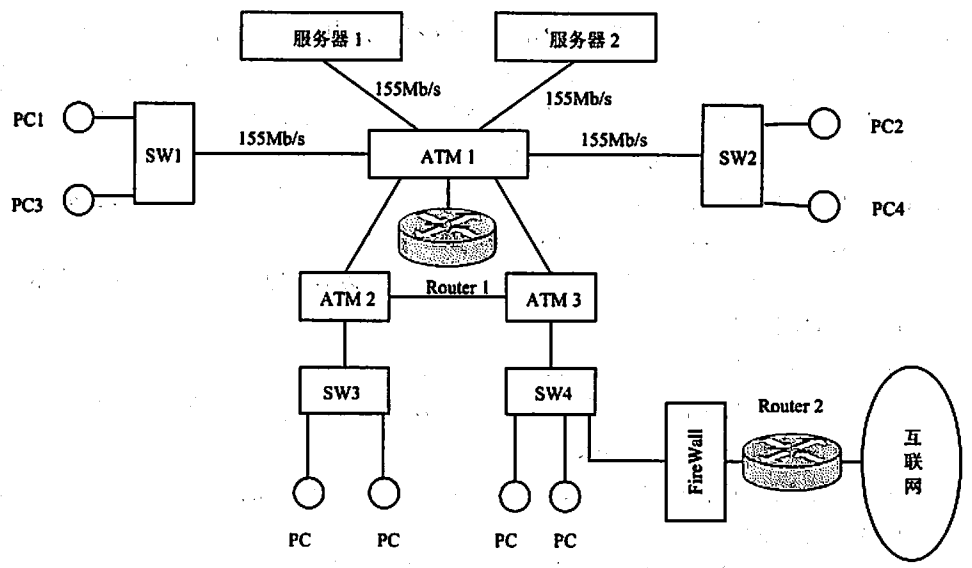


图 8.7 企业网络示意图

【问题】

1. 该企业网络的核心层采用了 ATM 技术，由 3 台 ATM 交换机互联构成。试对 ATM 网络技术的主要特点、协议分层结构和优点作简要叙述(控制在 100 个字以内)。

2. PC1~PC4 按 100Mb/s 的以太网协议运行，PC1 和 PC2 划分在一个虚拟网之中(VLAN1)，PC3 和 PC4 划分在另一个虚拟网之中(VLAN2)，试述 PC1 和 PC2 之间 IP 包通信的全过程(控制在 100 个字以内)。

3. 图中用了两台路由器，Router1 和 Router2，简述路由器的技术特点，并说明 Router1 和 Router2 在本网中的作用(控制在 100 个字以内)。

分析：我们知道，ATM 使用的是异步传送模式，以 53 个字节的等长信元为单位，进行信元交换。ATM 是一种分层体系结构。ATM 分层由 OSI 参考模型的第一层(物理层)和第二层(数据链路层)构成。其数据链路层又可以分为：ATM 层、AAL(ATM 适配层)SAR(分段和重新装配子层)子层、AAL CS(汇聚子层)子层。ATM 本质上是一种数据链路实现，以面向连接方式实现数据传送。ATM 综合了线路交换和分组交换的优点，并且支持 QoS(服务质量)。

PC1 和 PC2 在同一个 VLAN 之中，因此 PC1 与 PC2 要进行通信时，PC1 首先从 LES (局域网仿真服务器)获得 PC1 的地址，LES 将登记 PC2 的地址返回 PC1，然后它们就建立起连接，并完成 IP 包的传送。

路由器工作在 OSI 参考模型的第三层(网络层)，负责不同网络间的路由寻址、数据转发等，其安全性高于网桥，可以隔断广播域。Router1 为核心层路由器，实现不同虚拟网络 VLAN 之间的路由计算、数据转发。Router2 为边界路由器，负责企业内部网(Intranet)和因特网(Internet)之间的路由计算、数据转发。

答案：略。

例 2　阅读以下有关网络结构的说明，回答问题 1~问题 3。(2002 年下午试题三)

【说明】

如图 8.8 所示，GSW 为千兆以太网交换机，内设 ATM 模块。SW1 为 100/1000Mb/s 以太网交换机，SW2 为 ATM/100Mb/s 以太网交换机，RT 为中心路由器；S1 和 S2 为服务器，分别经千兆以太网卡和 155M ATM 网卡与 GSW(千兆以太网交换机)和 ATM 交换机相连，PC1、S1、S2、PC4 划分在 VLAN1 中，PC2、PC5 划分在 VLAN2 中，PC3、PC6 划分在 VLAN3 中。

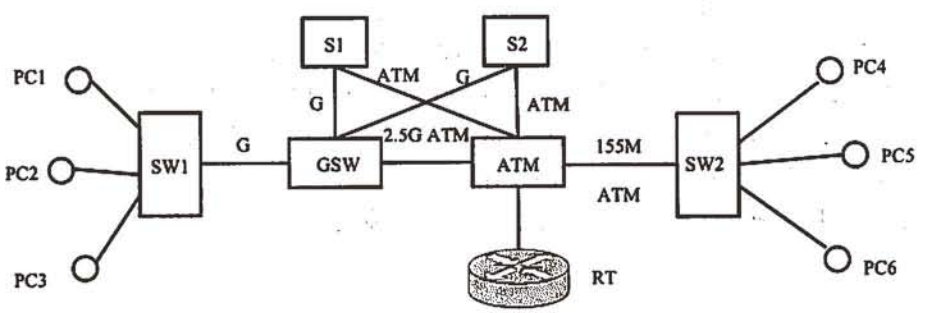


图 8.8　ATM 网络示意图

【问题】

1. 为了实现 VLAN1，VLAN2 和 VLAN3 的虚拟网络划分，在 ATM 和 RT 路由器中应设置哪几种服务协议(如 BUS)?

2. 试述从 PC1 发送一个 IP 包到 PC4 数据封装与解封的全过程。

3. 试述从 PC1 发送一个 IP 包到 PC2 的路由计算过程和传送路径。

分析：在 ATM 仿真 LAN(LANE)时，需要使用执行转换及管理过程的软件，这些软件驻留在 ATM 网络的不同设备中。两个主要的组件是 LAN 仿真客户(LEC)以及 LAN 仿真服务器(LES)。此外，还需要广播及未知服务器(BUS)和 LAN 仿真配置服务器(LECS)。

由于 PC1 和 PC4 在同一个 VLAN 之中，所以 PC1 与 PC4 进行通信时，PC1 首先从 LES(局域网仿真服务器)获得 PC4 的地址，而 LES 将已登记 PC4 的地址返回 PC1。然后它们就建立起连接，具体的 IP 数据包发送过程为：①PC1 把 IP 包封装成链路层数据帧，经 SW1 传送到 GSW，经 GSW 的 ATM 接口向 ATM 交换机传送；②此时链路数据帧再封装成 ATM 信元，从 SW2 向 PC4 传送时再由信元解封变成链路帧；③最后再从链路数据帧解封提取出 IP 包到 PC4。

而对于 PC1 和 PC2 的通信，PC1 首先要向 LES(局域网仿真服务器)询问 PC2 地址；由于 PC2 和 PC1 不在同一个 VLAN 中，所以 LES 要再向 LECS(LAN 仿真配置服务器)询问 PC2 在何处。然后，LECS 向 LES 回答，LES 把 PC2 的地址告知 PC1。最后，PC1 把 IP 包从 SW1 一个端口经 PC2 所在端口传送到 PC2。

答案：略。

8.3.3 同步练习

1. 帧中继与 X.25 一样，也提供虚拟电路服务，支持的虚拟连接可分为__(1)__和__(2)__两种。帧中继和 X.25 之间的差别在于帧中继只使用两个通信层：__(3)__和__(4)__。这两层分别对应于 OSI 模型中的__(5)__和__(6)__。

2. 说明 ATM 的分层结构以及每层的功能。

8.3.4 同步练习参考答案

1. (1) 交换型(SVC)　(2) 永久型(PVC)　(3) 物理层
   (4) 链接访问协议(LAPF)　(5) 物理层　(6) 数据链路层

2. ATM 采用了一个四层结构，称为 ATM 协议参考模型。物理层负责将信元转换成比特(bit)，用于在物理媒介上传输，并包括 ATM 的电子及物理连接。ATM 层的基本职责是以适当的方式在发送方和接收方之间交换信元；ATM 层上的基本数据单元是“信元”。ATM 适配层(ATM Adaptation Layer，AAL)的 SAR 子层，主要负责接收从 CS 发送来的任何信息，并构成 48 个字节的单元，作为 ATM 信元载荷。而 AAL 的 CS 子层，主要负责接收来自上层(例如 IP 数据)的 PDU，并一般通过增加负荷进行适配，以提交 SAR。

8.4 远程安全访问

8.4.1 考点辅导

在拨号或者 VPN 环境中部署远程接入解决方案时，需要考虑远程访问的管理、维护等问题。为了解决这些问题，需要仔细考虑远程接入的认证、授权和统计(AAA)。认证将解决每个用户如何进行确认的问题；授权将处理单个用户通过认证之后所拥有的权限问题；而记账方法则与使用问题相关联。

现在，就让我们来详细了解远程访问以及 VPN 网络完全技术。

8.4.1.1 远程访问服务器

远程访问是指地理位置分散的用户通过某种连接方式访问远程资源。远程访问一般采用各种类型的拨号连接或广域网连接的方式接入网络。远程访问的建立与局域网不同，局域网是由企业或学校独立完成传输网络的建设，因此传输网络的传输速率可以很高。而构建于广域网的远程访问由于受各种条件的限制，需借助公共传输网络。

RAS 是远程访问服务器(Remote Access Server)的缩写，也称为远程接入服务器。

1. 功能

远程访问服务器(RAS)提供了集中的网络功能。用户通过 RAS 可以接入到多种网络，如：PSTN(公共交换电话网)、ISDN(综合业务数字网)、GSM(环球移动通信)、DSL(数字用户线路)型接入网及固定线路网等；RAS 同时提供对局域网(LAN)或广域网(WAN)的适配功能，并且是网络提供增值服务的一个实时部分。RAS 所处的地位，使它成为完成用户接入认证、提供特定网络服务和接入计费统计功能的重要组成部分。

RAS 的主要特点：它是主要的分布网络部件，通常处于不同网络位置；种类繁多，在一个接入系统中可能出现多个供应商的多种产品。

远程访问服务器的上述特点使得建立一个统一的服务管理中心变得非常重要。因此，IETF(Internet Engineering Task Force)提出了 RADIUS(Remote Authentication Dial In User Service，远程验证拨号用户服务)协议——通过此协议，RAS 将用户验证请求和计费信息通过网络传给服务管理中心，并根据应答完成相应的功能。

RADIUS 的两个相关文档是 RFC 2138 和 RFC 2139。RADIUS 协议定义了一个严格的通信规范，包括通信包的数据格式、请求和应答方式、安全措施等。RADIUS 也提供了一个可扩展的应用规范，开发者可根据这个应用规范完成通用的基本功能，并可拓展其他专用的应用。

RAS 服务器需要对远程接入的用户进行登记、识别，对不同的用户进行分类，赋予其不同的访问权限。RAS 对用户上网进行记录和数据采集，以便生成账单、日志、审计等。这就是通常所说的 AAA 管理(Authentication,Authorization,Accounting，认证、授权、统计)。

对于接入层的 AAA 管理，曾经出现过多种协议规范以及在其之上的应用。这些协议和应用有一个共同的特点，就是它们都是由接入设备供应商开发的。原因就是接入层的认证、授权、记账与网络接入设备有密不可分的关系。现在 RADIUS 协议已经成为标准的

AAA 管理通信协议，被广泛使用。

2. 机制

当前，RADIUS 协议采用 Client/Server 的模式：

- 远程访问服务器(RAS)作为 RADIUS 的客户机 将用户接入的基本信息传递给 RADIUS 服务器，并接收 RADIUS 服务器的应答信息，对用户接入请求作相应的操作。
- RADIUS Server 作为 RADIUS 服务器 应答 RADIUS 客户的请求，验证用户身份或统计用户上网资料，并返回用户授权信息；或者作为代理客户机——作为别的 RADIUS 服务器(或其他类型的认证服务器)的客户机，对其本身的客户请求进行转发、应答。

从用户开始与 RAS 通信到用户中断连接的这个时期内，叫做用户远程访问的一个会话过程(session)。而 RADIUS 协议包括 RADIUS 和 RADIUS Accounting 两部分。在一个用户请求远程访问的会话过程中，至少应该存在两种相互独立的 RADIUS 通信过程：一种是验证过程(Authentication Process)；另一种是统计过程(Accounting Process)。

验证过程通常发生在用户与 RAS 建立网络连接之前，在一个 session 内，至少包括一个验证过程。RADIUS 服务器和客户机(RAS)通过验证过程完成对用户的身份鉴别，授权给所请求的服务。

统计过程在一次 session 中通常会进行两次：一次发生在 session 建立连接时，被称为会话开始统计(session start accounting)；另外一次发生在 session 结束之前，被称为会话结束统计(session stop accounting)。RADIUS 协议规定在同一个 session 中，两次统计过程用一个惟一的标识(acct-session-id)关联起来。

在用户访问 RAS 的一个 session 中，RADIUS 的通信过程是这样的：

(1) 一个被设置为需要验证访问的 RAS，当用户接入 RAS 的时候，它将为用户提供一个输入模式，使用户可以输入自己的账号和密码。这个过程通常以终端方式连接，即还没有进行数据链路层的协议连接，用户设备(一般为 PC)以远程终端方式挂接在 RAS 服务器上。

(2) RAS 得到用户输入的账号和密码后，运行 RADIUS 客户程序，生成一个 RADIUS 数据包，其中包括的属性字段有：用户名、用户密码、RAS 的 IP 地址、RAS 的端口号等信息。在用户密码字段中，RADIUS 协议规定使用 MD5 算法进行加密。RAS 将这个数据包发给 RADIUS 服务器，这个数据包称为 Access-Request Packet。

(3) “Access-Request Packet”通过网络从 RAS 传给 RADIUS 服务器，并等待应答。如果 RAS 在一段时间内未受到应答，则作如下处理：

第一步：重试。重复将 Access-Request Packet 发向同一个 RADIUS 服务器。

第二步：更换服务器。若超过重试次数，则更换 RADIUS 服务器，重复第一步。

第三步：连接出错。前两步失败，则认为 RADIUS 网络连接失败。

(4) 当 RADIUS 服务器接收到客户(RADIUS Client)的请求(Access-Request)时，将作如下处理：

第一步：进行客户认定。只有合法客户的请求，才作处理。具体方法是：检查客户资料数据库，客户资料数据库包括合法客户的 IP 地址、对称密钥、客户类型等。

第二步：如果客户是合法的，RADIUS 服务器通过用户名的格式，判断用户是否为本地用户。

(5) 当用户不满足以上的必要条件时，RADIUS 服务器向客户(RAS)发送一个 Access-Reject 数据包。Access-Reject 数据包中可以包括字符串提示信息。RAS 接收到 Access-Reject 应答后，就拒绝用户连接请求，并向用户标明拒绝访问的提示信息。

(6) 当所有条件均满足时，RADIUS 服务器将此用户的访问属性值(授权属性)放入 Access-Accept 数据包中，发送给 RAS。用户访问属性包括：服务类型(Service-Type：PPP，SLIP，telnet，rlogin)、与服务有关的参数(IP address，subnet mask，MTU，compress，hostname)、访问约束条件(filter-id，IP-Pool)等。RAS 接收到 RADIUS 服务器的 Access-Accept 数据包后，根据授权属性信息，提供规定的接入服务。

以上的(1)~(6)步，完成验证和授权过程。

(7) RAS 完成第 6 步后，马上向 RADIUS 服务器发送会话开始(session start)统计请求 Accounting-Request。其中，包含用户上网所用的资源信息，如：用户名、主叫、被叫号码、RAS 的 IP 地址、占用 RAS 的端口、分配的 IP 地址、服务类型及相关参数等信息。RADIUS 服务器接收 Accounting-Request，进行记录并发送 Account-Response 应答。

(8) 用户连接中断，可能是用户主动断开连接，也可能因为线路或设备的原因非正常中断。

(9) 用户连接中断后，RAS 向 RADIUS 服务器发送会话结束(session stop)统计请求 Accounting-Request。其中，包含了更详细的统计信息，如：用户名、主叫、被叫号码、RAS 的 IP 地址、占用 RAS 端口、分配的 IP 地址、服务类型及相关参数、用户在会话过程中上传字节数、下传字节数、上传数据包数、下传数据包数等。RADIUS 服务器接收 Accounting-Request，进行记录并发送 Account-Response 应答。

(10) 将 session-start 和 session-stop 统计信息合在一起可生成一条用户接入层上网记录。

以上就是远程访问服务器时 AAA 的整个实现过程。通过认证、授权、统计的手段，网络管理人员可以通过 RAS 和 RADIUS 服务器上的日志、资料，对网络攻击、安全漏洞等做好预测、监控。

8.4.1.2　虚拟专用网

1. 功能

伴随 Internet 的快速发展，数百万人将他们的家用计算机连到了 Internet 上，成千上万的组织机构也连了进去，Internet 已经发展成为一个巨大的商业冒险场所。

随着企业的收购和合并愈演愈烈，再加上企业本身的发展壮大与跨国化，每家企业的分支机构不仅越来越多，而且它们的网络基础设施互不兼容也更为普遍。因此，企业的信息技术部门在连接分支机构方面也感到日益棘手。

企业之间的合作及企业与客户之间的联系也日趋紧密，这些合作和联系是动态的，总是处在变化和发展之中。这种关系也要靠网络来维持和加强，这不但带来了网络的复杂性，还带来了网络的安全性问题。

虚拟专用网(Virtual Private Networking，VPN)技术就是在这种形势下应运而生的。VPN 技术将 Internet 作为计算机网络主干的一种网络模式。其基本特点就是化公为私，使每个企

业可以临时从公用网中挖走一部分地盘供自己专用。于是，企业网络想连接到哪里都可以，保密性、安全性、可管理性的问题也容易解决了，而且还可以降低网络的使用成本。据估计，VPN 可以使企业的远程访问和分支机构连接成本降低 50%以上。

打个比方说，如果一个外企员工在驻北京办事处工作，其公司总部却在新加坡。只能通过电话拨号到新加坡的亚太总部来收发电子邮件和访问公司的内部 Web。电话费用非常高，而且通信速度也不理想。但是，假如新加坡亚太总部已经和 Internet 联网，那么只要驻北京办事处申请一个本地的 Internet 账号，然后借助 Internet 这张大网，就可以与亚太总部联上了。这样不仅可以在短时间内与公司联网，而且只需付出低廉的本地电话费和 Internet 使用费。至于通信安全和联网速度，虚拟专用网 VPN 还可以提供通信安全和联网速度保障。VPN 的效果相当于在 Internet 里自动拉一条虚拟专线，这条专线叫隧道(tunnel)。

2. 机制

在了解 VPN 的功能之后，我们将从其组成要素以及具体实现两方面描述 VPN 的实现机制。

(1) VPN 的基本要素

为了形成 VPN 中的隧道，需要具备的资源有：隧道开通器(TI)、有路由能力的公用网络、一个或多个隧道终止器(TT)、必要时增加一个隧道交换机以增加灵活性。

隧道开通器的任务是在公用网中开出隧道。有多种网络设备和软件可完成此项任务，例如：配有模拟式调制解调器 PC 卡和 VPN 型拨号软件的计算机。

隧道终止器的任务是使隧道到此终止，不再继续向前延伸。也有多种网络设备和软件可完成此项任务，例如：专门的隧道终止器；企业网络中的隧道交换机。

VPN 网络中通常还有一个或多个安全服务器。安全服务器除提供防火墙和地址转换功能之外，还通过与隧道设备的通信来提供加密、身份查验和授权功能。它们通常也提供各种信息，如带宽、隧道端点、网络策略和服务等级。通过软件或模块升级，现有的网络设备可以增加 VPN 能力。一个有 VPN 能力的设备可以承载多项 VPN 应用。

(2) VPN 的实现

VPN 的建立可以基于几种不同的网络协议，其中最常见的是利用 PPTP 协议的 VPN 工作方式。

基于 PPTP 协议(点对点密道协议)的网络连接方式的 VPN，允许一台客户机通过一个公共网络(例如，Internet 网)建立一个秘密的多协议虚拟网络。因此，它可以使得公司远端的员工通过 Internet 而不是直接拨号连接公司的网络。这就是说，通过 PPTP 的封装，使非 IP 网络获得 Internet 通信的优点。PPTP 是微软和其他厂家支持的标准，它是 PPP 协议的扩展，可以通过 Internet 建立多协议 VPN。

VPN 模仿点对点连接技术，依靠 Internet 服务提供商(ISP)和其他的网络服务提供商(NSP)在公用网中建立自己专用的“隧道”，让数据包通过这条隧道传输。对于不同的信息来源，可分别给它们开出不同的隧道。于是，兼容性问题、不同的服务质量要求以及其他的麻烦都迎刃而解。

PPTP 协议是一种第二层隧道协议。为了传输来自不同网络的数据包，最普遍使用的方法是先把各种网络协议(IP、IPX 和 AppleTalk 等)封装到 PPP 里，再把这整个数据包装入隧道协议里。这种双层封装形成的数据包需靠第二层协议进行传输，所以称之为“第二层隧

道”。另一种方法是把各种网络协议直接装入隧道协议中，由于形成的数据包需靠第三层协议进行传输，所以称之为“第三层隧道”。

除了基于 PPTP 模式的 VPN 之外，VPN 可以基于以下的几种协议。

① GRE——通用路由封装

(GRE)协议是由 Cisco 和 Net-smiths 等公司 1994 年提交给 IETF 的，相关文档为 RFC1701 和 RFC1702。目前有多数厂商的网络设备均支持 GRE 隧道协议。

GRE 规定了如何用一种网络协议去封装另一种网络协议的方法。GRE 的隧道由两端的源 IP 地址和目的 IP 地址来定义，允许用户使用 IP 包封装 IP、IPX、AppleTalk 包，并支持全部路由协议(如 RIP2、OSPF 等)。通过 GRE，用户可以利用公共 IP 网络连接 IPX 网络、AppleTalk 网络，还可以使用保留地址进行网络互联，或者对公网隐藏企业网的 IP 地址。GRE 只提供了数据包的封装，没有加密功能来防止网络侦听和攻击，所以在实际环境中经常与 IPsec 一起使用，由 IPSec 提供用户数据的加密，从而给用户提供更好的安全性。

② L2TP——第二层隧道协议

除 Microsoft 外，还有一些厂家也做了许多开发工作。PPTP 能支持 Macintosh 和 Unix，而 Cisco 的 L2F(Layer2 forwarding)也是一个隧道协议。Microsoft、Cisco 和其他一些网络厂商正一起努力使 L2F 与 PPTP 融合，产生一个新的 L2TP 协议。L2TP 和 PPTP 十分相似，因为 L2TP 有一部分就是采用 PPTP 协议，这两个协议都允许客户通过其间的网络建立隧道。L2TP 还支持信道认证，但它没有规定信道保护的方法。

③ IPsec——IP Security

开发这个协议的目的是要解决当前协议中存在的一些缺点。IPsec 是由 IETF IP 安全性工作组定义的协议集，用于确保网络层之间的安全通信。该协议草案建议使用 IPsec 协议集保护 IP 网和非 IP 网上的 L2TP 业务，以及如何共同使用 IPsec 和 L2FP。下一小节将对 IPsec 作详细介绍。

④ SOCKs

SOCKs 协议是一个网络连接的代理协议，它使 SOCKs 一端的主机完全访问 SOCKs，而另一端的主机不要求 IP 直接可达。SOCKs 能对连接请求进行鉴别和授权，并建立代理连接和传送数据。SOCKs 通常用作网络防火墙，使 SOCKs 后面的主机能通过 Internet 取得完全的访问权，而避免了通过 Internet 对内部主机进行未授权访问。目前，有 SOCKs V4 和 SOCKs V5 两个版本，SOCKs V5 可以处理 UDP，而 SOCKs V4 则不能。

3. IP 隧道

“隧道”是封装的一种形象的说法。这两个术语之间的差别是：封装一般是将高层协议包装在低层协议的报头中的一种自顶向下的方法，而隧道一般是将下层协议放在高层协议内部进行传输的方法。使用隧道传递的数据(或负载)可以是不同协议的数据帧或包，隧道协议将这些数据帧或包重新封装在新的包头中发送。新的包头提供了路由信息，从而使封装的负载数据能够通过互联网传递。

例如，IP 数据包(第三层，网络层)通常包装在点到点协议(PPP)帧(第二层，数据链路层)中，然后发送点到点协议帧。而在隧道环境中，网间数据包交换(IPX)数据包(第三层，网络层)可以放到 PPP 协议帧(第二层，数据链路层)中，再将 PPP 协议帧放在 IP 数据包(第三层，网络层)中——整个数据包在发送之前再放到另一种帧内。

隧道在传统上一直是必要的，因为要传输的数据存在不能被所通过的网络理解的可能。比如，IPX 不能在像 Internet 这样的 IP 网络上直接传输。可以把 IPX 看做是汽车，把 Internet 看成是湖，我们不能开车通过湖。但是，如果把汽车放在渡轮(隧道协议)上，就可以把车子运过湖。今天，像 NetWare 和 SNA 这样的旧网络体系要在 Internet 中进行通信，则需要在网络层上转向 IP 协议。

通过隧道的建立，可实现以下功能：

- 将数据流量强制到特定的目的地。
- 隐藏私有的网络地址。
- 在 IP 网上传输非 IP 协议数据包。
- 提供数据安全支持。
- 协助完成用户基于 AAA 的管理。

IPsec 是 IETF(Internet Engineer Task Force)正在完善的安全标准，它把几种安全技术结合在一起形成一个较为完整的体系。通过对数据加密、认证、完整性检查来保证数据传输的可靠性、私有性和保密性。IPsec 由 IP 认证头 AH(Authentication Header)、IP 安全载荷封载 ESP(Encapsulated Security Payload)和密钥管理协议组成。

IPsec 在 IP 网络层上对数据包进行高强度的安全处理，提供数据源的验证、无连接数据完整性、数据机密性、抗重播和有限业务流机密性等安全服务。各种应用程序可以享用 IP 层提供的安全服务和密钥管理，而不必设计和实现自己的安全机制，因此减少密钥协商的开销，也降低了产生安全漏洞的可能性。IPsec 可连续或递归应用，在路由器、防火墙、主机和通信链路上配置，实现端到端安全、虚拟专用网络(VPN)和安全隧道技术。

IPsec 隧道模式使用安全方式封装，并加密整个 IP 包。然后对加密的负载再次封装在明文 IP 包头内通过网络发送到隧道服务器端。隧道服务器对收到的数据报进行处理，再去除明文 IP 包头，对内容进行解密之后，获的最初的负载 IP 包。负载 IP 包在经过正常处理之后，被路由器路由到目的 IP 地址所在的网络。

IPsec 支持的组网方式包括：主机之间、主机与网关、网关之间的组网。IPsec 还支持用户进行远程访问。IPsec 可以和 L2TP、GRE 等隧道协议一起使用，给用户提供更大的灵活性和可靠性。

8.4.2 典型例题分析

例 1 阅读以下说明，回答问题 1 和问题 2。(2003 年下午试题六)

【说明】

VPN 是通过公用网络 Internet 将分布在不同地点的终端联接而成的专用网络。目前大多采用 IPsec 实现 IP 网络上端点间的认证和加密服务。

【问题】

1. 某公司的网络拓扑结构如图 8.9 所示，采用 VPN 来实现网络安全。请简要叙述从公司总部主机到分支机构主机通过 IPsec 的通信过程。

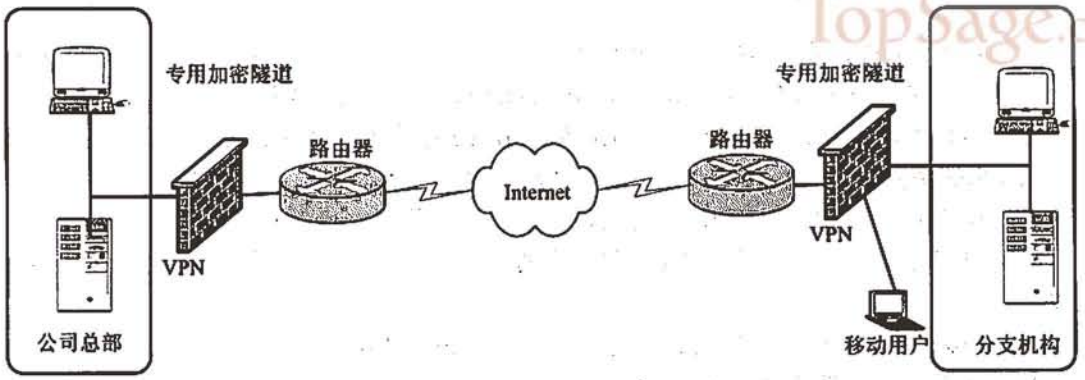


图 8.9　VPN 实现网络拓扑图

2. 某路由器的部分配置信息如下所示，请解释其中标有下划线部分的含义(“//”后为注释内容)。

```
*配置路由器信息
version 12. 0 //版本
hostname SecRouter//路由器名称
boot system flash c1700-osy56i-mz_120-3-T3.bin
//应用 IKE 共享密钥进行认证
//创建标识为“100”的 IKE 策略
crypto isakmp policy 100
hash md5                          (1)
authentication pre-share          (2)
//与远端 IP 为 172.16.2.1 的对等体的共享密钥为“mcns”
crypto isakmp key mcns address 172.16.2.1
//配置名为 1&2 的交换集，指定 esp-des 和 esp-md5-hmac 两种变换
crypto ipsec transform-Set 1&2 eSp-deS eSp-md5-hmaC
//配置加密图
//分配给该加密图集的名称：sharef，序号：10；
//指定用 IKE 来建立 IPSec 安全关联，以保护由该加密图条目所指定的数据流
crypto map sharef 10 ipsec-isakmp
set Deer 172.16.2.1               (3)
set transform-set 1&2             (4)
match address 151
//配置接口
interface serial0
ip address 172.16.1.1 255.255.255.252
ip access-group 101 in
crypto map sharef                  (5)
interface FastEthernet0
end
```

分析：

1. 根据图 8.9 中的网络结构，公司总部主机与分支机构主机之间采用 IPsec 协议进行 VPN 连接通信，需要经历隧道建立开始阶段、数据传输阶段以及隧道拆除阶段。整个通信

的过程如下:

(1) IPsec 过程启动 根据配置 IPsec 对等体(公司总部主机和分支机构主机)中的 IPsec 安全策略,指定要被加密的数据流,启动 IKE(Internet 密钥交换)过程。

(2) IKE 阶段 1 在该连接阶段,IKE 认证 IPsec 对等体,协商 IKE 安全关联(SA),并为协商 IPsec 安全关联的参数建立一个安全传输道路。

(3) IKE 阶段 2 IKE 协商 IPsec 的 SA 参数,并在对等体中建立起与之匹配的 IPsec SA。

(4) 数据传送 根据存储在 SA 数据库中的 IPsec 参数和密钥,在 IPsec 对等体间传送数据。

(5) IPsec 隧道终止 通过删除或超时机制结束 IPsec SA。

2. 问题中路由器的配置信息解析如下:

(1) 采用 md5 hash 算法。

(2) 采用预共享密钥认证方法。

(3) 指定允许的 IPsec 对等体的 IP 地址为 172.16.2.1。

(4) 此加密图使用交换集 1&2。

(5) 此接口使用名为 sharef 的加密图进行加密。

答案:略。

例 2 阅读以下有关网络设备安装与调试的叙述,分析设备配置文件,回答如下问题。(2001 年下午试题四)

【说明】

现以一台远程访问服务器(RAS,Remote Access Server)Cisco 2509、RJ45 为例来说明。

第一步,准备安装与调试所需的设备,主要包括 RASCisco 2509、RJ45 直通线,RJ45 9 针串口转换器、计算机。

第二步,硬件连接,RJ45 直通线一头插入 Cisco 2509 的 console 口,另一头接 RJ45 9 针串口转换器,再将转换器接到计算机的串口。

第三步,RAS 加电,在计算机上调用 Windows 98 下的超级终端程序,配置设备连接参数,以便进入 Cisco 设备的虚拟操作台。

第四步,输入 Cisco 2509 的 IOS 配置命令。

第五步,将调试完毕的设备连入本地网络,通过拨号验证配置是否正确。

【问题】

1. 在调用超级终端程序进行设备连接时,应该对设备的连接参数进行正确设置,参数主要包括串口数据传输率、数据位数、停止位数以及是否有奇偶校验。请给出正确的连接参数,以便进入 Cisco 设备的虚拟操作台,进行设备调试(控制在 100 个字以内)。

2. 在第四步中,进入虚拟操作台后,在 IOS 环境下输入了如下的配置,请解释(1)~(4)处标有下划线部分配置命令的含义(“◇”后为配置内容,“★”和“//”后为注释内容)。

```
★ 配置服务器信息
◇ hostname Cisco 2509 //服务器名称
◇ enable secret****** //特权口令
```

◇ ip domain-manl wxx.edu.cn //设置拨号服务器所属域名
◇ ip-name-server 202.112.77.2 //设置拨号服务器 DNS
(1)(此处有 3 条下划线)
◇ async-bootp subnet-mask 255.255.255.0
◇ async-bootp gateway 202.112.77.254
◇ async-bootp dns-server 202.112.77.2
★ 配置 Ether Port (略)
……
★ 配置动态分配的地址池
◇ ip local pool pool2509 202.112.79.1 202.112.79.8 //定义 IP 地址池
★ 配置 Asynchronous Interface
//异步口是 RAS 服务器上连接 modem，用于用户拨号的端口
◇ interface Group-Async 1　//对第一组异步接口进行配置，对异步口的配置可以按组，也可以按单个口
group-range 1 8 //划定 1 到 8 号异步口属于第一组
encapsulation pap //加载点到点协议
(2)(此处有 2 条下划线)
ansync dynamic address
ansync default address pool pool2509　//pool2509 的定义见“配置动态分配的地址池”部分
ppp authentication pap //设置 PPP 的验证方式为用户口令方式
★ 配置 router 信息
(3)(此处有 3 条下划线)
◇ router rip
network 202.112.77.0
network 202.112.79.0
★ 配置拨号服务器的缺省路由(略)
……
★ 配置存取用户组
◇ access-list 1 permit 202.112.77.0 0.0.0.255 //定义用户组的范围
★ 配置 Asynchronous PORT (略)
★ 配置 vty
◇ Iine vty 0 4 //配置虚拟终端
(4)(此处有 3 条下划线)
access-class 1 in //access-class 的定义见“配置存取用户组”
pasword ******
login

分析：

1. 要对 Cisco 公司的网络设备通过 CONSOLE(控制台)进行配置，则不管是交换机还是路由器等设备，都是用如下串口连接参数：

波特率 9600b/s、数据位 8 位、奇偶检验无、停止位 1 位。

2. 从路由器的配置信息，可以得到如下解析：

(1) 配置 RAS 拨号的用户网络配置信息。主要包括：用户默认子网掩码、默认网关、默认 DNS。当用户拨入时，服务器自动将配置信息传递给用户。

(2) 设定第一组异步口的用户 IP 地址自动分配。设置自动分配的 IP 地址来自于 IP 地址池 pool2509。

(3) 配置动态路由协议 RIP——路由信息协议。指定此网络设备需要宣告的路由信息，直接连到网段 202.112.77.0 和 202.112.79.0 的路由。

(4) 设置允许来自 202.112.77.0/24 网段的用户访问拨号服务器并配置用户登录所需的密码。

答案：略。

例 3 阅读以下说明，回答问题 1~问题 3。(2004 年下半年下午试题一)

【说明】

某公司规模扩大时要求：既要考虑保证目前土建装修的效果不被破坏，又要满足网络扩容和企业工作实际需求，同时还要保证投资不要过大。经过深入分析和研究对比，决定采用无线局域网组网来解决网络扩容的问题，网络拓扑如图 8.10 所示。

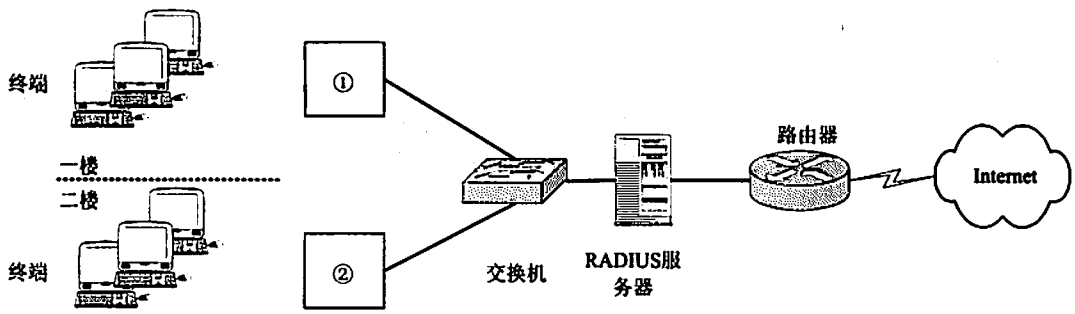


图 8.10 公司网络拓扑图

【问题】

1. 从工作的频段、数据传输速率、优缺点以及它们之间的兼容性等方面，对 IEEE 802.11a、IEEE 802.11b 和 IEEE 802.11g 进行比较。

2. (1) 请写出①处空缺的设备。

(2) 在①处所在局域网内的 PC 机或笔记本的 IP 地址有哪几种分配方式？在安装设备①时，如何配置这几种方式？

(3) 对 PC 机或笔记本中无线网卡进行配置时，“encryption”项的值如何确定？

(4) 配置完成后，采用什么命令测试该无线网是否连通？

3. 简述 WLAN 用户通过 RADIUS 服务器登录的过程。

分析：无线局域网(Wireless Local Area Network，WLAN)一种通过无线介质发送和接收数据的网络访问形式。WLAN 802.11 标准于 1997 年获得 IEEE 认可后，先后出现了 IEEE 802.11a、IEEE 802.11b、IEEE 802.11g 等标准。各种标准间的主要问题在于兼容性，尤其是 WLAN 间的漫游需要得到各种技术标准的一致支持。WLAN 标准不同，其数据传输速率、传输距离也有所不同。802.11a 扩充了 802.11 标准的物理层，规定该层使用 5GHz 的频带。该标准采用 OFDM(正交频分)调制技术，传输速率的范围为 6Mb/s ~ 54Mb/s。802.11b 规定采用 2.4GHz 频带，调制方法采用补偿码键控(CKK)，共有 3 个不重叠的传信道。其传输速率能够从 11Mb/s 自动降到 5.5Mb/s。802.11g 运行于 2.4GHz，网络达到了 54Mb/s 的高

传输速率。与有线网络相比，WLAN 具有安装便捷、使用灵活、易于扩展、价格便宜、辐射小等优点，可以应用于公共场所(如：机场、酒店、展厅的网络接入、企业移动办公系统、金融服务和旅游服务等)。

接入点(Access Point，AP)一般俗称为网络桥接器，顾名思义即是当做传统的有线局域网络与无线局域网络之间的桥梁，因此任何一台装有无线网卡的 PC 均可通过 AP 去分享有线局域网络甚至广域网络的资源。除此之外，AP 本身又兼具有网管的功能，可针对接有无线网络卡的 PC 作必要的控制。

要组建无线局域网，必须要有相应的无线网设备，这些设备主要包括：无线网卡、无线访问接入点、无线 HUB 无线网桥。几乎所有的无线网络产品中都自含无线发射/接收功能，且通常是一机多用，无线网卡主要包括：NIC(网卡)单元、扩频通信机和天线三个功能模块。

NIC 单元属于数据链路层，由它负责建立主机与物理层之间的连接；扩频通信机与物理层建立了对应关系，通过天线实现无线电信号的接收与发射。无线 HUB 既是无线工作站之间相互通信的桥梁和纽带，同时又是无线工作站进入有线以太网的访问点，负责管理其覆盖区域(无线单元)内的信息流量。覆盖彼此交叠区域的一组无线 HUB，能够支持无线工作站在大范围内的连续漫游功能，同时又能始终保持网络连接，这与蜂窝式移动通信的方式非常相似。另外，在同一地点放置多个无线 HUB，可以实现更高的总体吞吐量。无线网桥主要用于无线局域网或有线局域网之间的互联。当两个局域网无法实现有线连接或使用有线连接存在困难时，可使用无线网桥实现点对点的连接，在这里无线网桥起到了网络路由选择和协议转换的作用。

答案：

1. 802.11a 扩充了 802.11 标准的物理层，规定该层使用 5GHz 的频带。该标准采用 OFDM(正交频分)调制技术，传输速率范围为 6Mb/s~54Mb/s。而 802.11b 则规定采用 2.4GHz 频带，调制方法采用补偿码键控(CKK)，共有 3 个不重叠的传输信道。其传输速率能够从 11Mb/s 自动降到 5.5Mb/s。802.11g，运行于 2.4GHz，网络达到了 54Mb/s 的高传输速率。

2. (1)设备名称是 AP(或访问接入点(Access Point，AP))。(2)静态或动态分配，在动态分配时，需要具备 DHCP 功能。(3)encryption 值与无线 HUB 设置的值相同；当无线 HUB 的 encryption 项选择 disable 时，网卡上的“encryption”项的值可以设置为“无”。(4)使用 ping 命令。

3. AP 首先使用“Access-Require”数据包向 RADIUS 服务器提交用户信息，其中包括用户名、密码等信息。然后，RADIUS 服务器对用户名和密码的合法性进行检验，要求进一步对用户认证，也可以对 AP 进行类似的认证。最后，RADIUS 服务器作出决定：如果合法，给 AP 返回“Access-Accept”数据包，允许用户进行下一步工作；否则返回“Access-Reject”数据包，拒绝用户访问。

8.4.3　同步练习

1. 远程访问服务所使用到的 AAA 技术中的 3 个 A 分别指代什么？

2. 目前，认证和记账系统使用最多的一种 C/S 模式的协议是 RADIUS。某 ISP 为了集中对网络设备(诸如路由器、交换机、监控系统等)的管理，采用了 RADIUS 远程访问认

证的机制，请简述网管通过 RADIUS 服务器登录网络设备(比如路由器)的验证和授权过程。

8.4.4 同步练习参考答案

1. 这里的3个A分别指代的是：Authentication，认证；Authorization，授权；Accounting，记账。

2. 略。

8.5 办公室个人手持电话系统(PHS)

8.5.1 考点辅导

8.5.1.1 PHS 系统简介

PHS 系统是日本提出的个人手持电话系统(Personal Handyphone System)，PHS 属于微蜂窝、高频段、低发射功率的系统。PHS 系统是于 1993 年由日本邮政省组织通信行业的各大公司、研究机构共同开发的。PHS 系统具有双向呼叫、越区切换和漫游的功能，并支持 ISDN 业务。

PHS 系统的主要技术参数如下：

- 频段　1900 MHz ~1920 MHz。
- 空中接口　BCR28V2。
- 射频信道间隔　300kHz。
- 双工方式　TDD。
- 多址方式　TDMA。
- 语音编码技术　32 Kb/s ADPCM。
- 信道分配方式　DCA。
- 调制方式　π/4 DQSK。

8.5.1.2 PHS 系统的功能特性

PHS 系统的设计理念是对 PSTN 的无绳体现。采用 PHS 组建无线市话网络，可以充分利用现有固定电话网的交换、传输以及线路资源，具有投资少、建设周期短、组网灵活方便、市场占领迅速等诸多优点。

PHS 系统与移动通信系统相比，有以下几点独特之处：

- 采用动态信道分配，无需频率规划，大大提高了频率资源的利用率。
- 单位面积内支持高话务密度。
- 采用微蜂窝技术，基站设备小，便于网络优化及话务调整。
- 语音编码采用 32 Kb/s ADPCM 方式，语音质量高。
- 支持 32 Kb/s 数据通信业务，同时使用两个 32 Kb/s 信道可使速率达到 64 Kb/s。
- 采用自适应阵列天线，将优质信号集中于目标用户位置。
- 基站功率低、覆盖范围小，可开发定位、跟踪、报警等增值业务。

- 低功率手机，延长了电池使用时间，降低了辐射。
- 兼有有线系统的低价位和蜂窝系统的可移动性。

由于 PHS 基站(基站是网络组成的最小单元)容量小，覆盖范围有限，所以需要相当数量基站的支撑，才能形成一定规模的用户群，并提供良好的服务。信号的覆盖、信道的切换是影响其发展的最大障碍。数目庞大的基站直接面对用户，因此基站网络覆盖质量如何决定了整个网络的服务质量。

PHS 系统信号穿透能力较弱，特别是经过建筑物的阻挡之后，信号的损伤更大。这样往往容易造成室内覆盖效果不佳，影响 PHS 业务的最终效果。因此，在进行 PHS 基站建设时，应考虑在原有大功率基站的基础上，穿插一些小功率基站和室内基站，以增强建筑密集区域的覆盖效果，消除盲点。

8.5.2　典型例题分析

例　阅读以下说明，回答如下问题。

【说明】

PHS 无线接入是指从交换节点到用户终端之间部分或全部采用了无线手段。典型的无线接入系统主要由控制器、操作维护中心、基站、固定用户单元和移动终端等几个部分组成。

【问题】

请说明这些组成部分的各个功能。

分析：对于 PHS 系统的应用，控制器的主要功能是处理用户的呼叫(包括呼叫建立、拆线等)、对基站进行管理。同时，控制器通过基站进行无线信道控制、基站监测和对固定用户单元及移动终端进行监视和管理。

操作维护中心负责整个无线接入系统的操作和维护，其主要功能是对整个系统进行配置管理，对各个网络单元的软件及各种配置数据进行操作。在系统运转过程中对系统的各个部分进行监测和数据采集；对系统运行中出现的故障进行记录并报警。

而基站则通过无线收发机提供与固定终端设备和移动终端之间的无线信道，并通过无线信道完成语音呼叫和数据的传递。控制器通过基站对无线信道进行管理。基站与固定终端设备和移动终端之间的无线接口可以使用不同技术，并决定整个系统的特点，包括所使用的无线频率。

固定终端设备为用户提供电话、传真、数据调制解调器等用户终端的标准接口。它与基站通过无线接口相接，并向终端用户透明地传送交换机所能提供的业务和功能。固定终端设备可以采用定向天线或无方向性天线。采用定向天线直接指向基站方向可以提高无线接口中信号的传输质量、增加基站的覆盖范围。

移动终端从功能上可以看做是将固定终端设备和用户终端合并构成的一个物理实体。由于它具备一定的移动性，因此支持移动终端的无线接入系统除了应具备固定无线接入系统所具有的功能外，还要具备移动性管理等蜂窝移动通信系统所具有的一定的功能。

答案：略。

8.5.3 同步练习

1. 简述无线接入的实现主要基于哪几种类型的技术。

2. “小灵通”又叫无线市话，英文缩写是__(1)__，最早由__(2)__(国家)提出。它采用__(3)__技术，是高频段、低发射功率的系统。“小灵通”具有__(4)__、越区切换和__(5)__的功能，并支持ISDN业务。“小灵通”手机以无线的方式接入本地电话网，使传统意义上的固定电话，不再固定在某个位置。

8.5.4 同步练习参考答案

1. 蜂窝技术、数字无绳技术、点对点微波技术、卫星技术。
2. (1) PHS (2) 日本 (3) 微蜂窝(信道) (4) 双向呼叫 (5) 漫游

8.6 网络互联设备

8.6.1 考点辅导

8.6.1.1 中继式 HUB

集线器是最简单的网络连接设备，属于数据通信系统中的基础设备，集线器的英文名称是 “HUB” —— 英文“HUB”是“中心”的意思。集线器(HUB)工作在局域网(LAN)环境，应用于OSI参考模型的第一层，因此又被称为物理层设备。集线器内部采用了电器互联，当维护LAN的环境是逻辑总线或环型结构时，完全可以用集线器建立一个物理上的星形网络结构或树形网络结构。

1. 功能

集线器实际上就是中继器的一种，其区别仅在于集线器能够提供更多的端口服务，所以集线器又叫多口中继器。

集线器的主要功能是对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有节点集中在以它为中心的节点上。集线器主要是以优化网络布线结构，简化网络管理为目标而设计的。集线器是对网络进行集中管理的最小单元，像树的主干一样，它是各分枝的汇集点。

以集线器为节点中心的优点是：当网络系统中某条线路或某节点出现故障时，不会影响网上其他节点的正常工作，这也是集线器刚推出时与传统的总线网络的最大的区别和优点，因为它提供了多通道通信，大大提高了网络通信速度。尤其是现代双速自适应以太网集线器，由于内置了可以实现内部 10Mb/s~100Mb/s 网段间相互通信的交换模块，使得这类集线器完全可以在以该集线器为节点的网段中实现各节点之间的通信交换，有时大家也将此类交换式集线器简单地称之为“交换机”。

但是，集线器由于自身的因素，也有先天的不足，主要体现在如下几个方面：

(1) 用户带宽共享，带宽受限

集线器的每个端口并没有独立的带宽，而是所有端口共享总的背板带宽，用户端口带宽较窄，且随着集线器所接用户的增多，用户的平均带宽不断减少，不能满足当今对网络带宽有严格要求的网络应用，如多媒体、流媒体应用等环境。

(2) 广播方式，易造成网络风暴

集线器是一个共享设备，其主要功能是对信号进行放大和中转。不具备自动寻址能力(即不具备交换作用)，所有传到集线器的数据均被广播到与之相连的各个端口，容易形成网络风暴，造成网络堵塞。

(3) 非双工传输，网络通信效率低

集线器的同一时刻每一个端口只能进行一个方向的数据通信，而不能像交换机那样进行双向双工传输，网络执行效率低，不能满足较大型网络的通信需求。

2. 机制

依据 IEEE 802.3 协议，集线器随机选出某一端口的设备，并让它独占全部带宽，与集线器的上联设备(交换机、路由器或服务器等)进行通信。集线器在工作时具有以下两个特点。

首先，集线器只是一个多端口的信号放大设备，工作中当一个端口接收到数据信号时，由于信号在从源端口到 HUB 的传输过程中已有了衰减，所以 HUB 便将该信号进行整形放大，使被衰减的信号再生(恢复)到发送时的状态，紧接着转发到其他所有处于工作状态的端口上。从 HUB 的工作方式可以看出，它在网络中只起到信号放大和重发作用，其目的是扩大网络的传输范围，而不具备信号的定向传送能力，是一个标准的共享式设备。

其次，集线器只与它的上联设备(如上层 HUB、交换机或服务器)进行通信，同层的各端口之间不会直接进行通信，而是通过上联设备再将信息广播到所有端口上。由此可见，即使是在同一 HUB 的不同两个端口之间进行通信，也必须要经过两步操作：第一步是将信息上传到上联设备；第二步是上联设备再将该信息广播到所有端口上。不过，随着技术的发展和需求的变化，许多 HUB 在功能上进行了拓展，加入了一些交换技术，使得集线器不再受这种工作机制的影响。

目前，集线器和交换机之间的界限已变得模糊。比如，交换式集线器有一个核心交换式背板，采用一个纯粹的交换系统代替传统的共享介质中继系统。

8.6.1.2　L2、L3、L4 及多层交换机功能和机制

1. L2 交换机功能和机制

L2(二层)交换技术发展比较成熟；二层交换机属数据链路层设备，可以识别数据包中的 MAC 地址信息，根据 MAC 地址进行转发，并将这些 MAC 地址与对应的端口记录在自己内部的一个地址表中。具体的工作流程如下：

(1) 当交换机从某个端口收到一个数据包时，它先读取该包头中的源 MAC 地址，这样它就知道源 MAC 地址的机器是连在哪个端口上的。

(2) 再去读取包头中的目的 MAC 地址，并在地址表中查找相应的端口。

(3) 如地址表中有与这目的 MAC 地址对应的端口，则把数据包直接复制到这端口上。

(4) 如地址表中找不到相应的端口则把数据包广播到所有端口上，当目的机器对源机器回应时，交换机又可以学习到这个目的 MAC 地址与交换机的哪个端口对应，在下次传

送数据时就不再需要对所有端口进行广播了。

二层交换机不断地循环这个过程，这样就可以学习到全网的 MAC 地址信息，二层交换机就是这样建立和维护它自己的地址表。

从二层交换机的工作原理可以得知二层交换机有这样的特点：

- 由于交换机对多数端口的数据进行同时交换，这就要求具有很宽的交换总线带宽，如果二层交换机有 N 个端口，每个端口的带宽是 M，交换机总线带宽超过 $N \times M$，那么这交换机就可以实现线速交换。
- 学习端口连接的机器的 MAC 地址，写入地址表，地址表的大小影响着交换机的接入容量。
- 二层交换机一般都含有专门用于处理数据包转发的 ASIC(Application Specific Integrated Circuit)芯片，因此转发速度可以做到非常快。

二层交换机与集线器(HUB)相比，其优点是非常突出的，试想，一个有 100 人的工作组使用集线器共享一个半双工的 10M 网段，那么平均每个人只有分配到 100K 左右的带宽；如果是用全双工的交换机的话，那么每端口的带宽是 20M，相差甚大。二层交换机使得在每个网段上可以提供更多的主机数。然而，二层交换机也和网桥一样有它们共同的局限性，网络的广播数据会随着网段上主机数目的增加而增加；广播也影响着主机传输数据，STP 限制、收敛速度慢和冗余链路封闭的问题仍然存在。

2. L3 交换机功能和机制

近年来，L3(三层)交换技术应用得越来越广，通过使用三层交换机可以使得网络构造变得丰富，而且可以获得很好的网络质量。下面将通过一个简单的网络来看看三层交换机的工作过程。

假设：有两台主机(分别是主机 A、主机 B)挂接在三层交换机上。比如主机 A 要给主机 B 发送数据，则三层交换机的工作过程为：

(1) 已知目的 IP，那么主机 A 就用其本身的子网掩码与该目的 IP 相与，取得目的网络号，判断目的 IP 是否与自己在同一网段。

(2) 如果在同一网段，但不知道转发数据所需的 MAC 地址，主机 A 就发送一个 ARP 请求，主机 B 返回其 MAC 地址；然后，主机 A 用此 MAC 封装数据包并发送给交换机，交换机起用二层交换模块，查找 MAC 地址表，将数据包转发到相应的端口。

(3) 如果目的 IP 地址不是同一网段的，那么主机 A 要实现和主机 B 的通信，主机 A 就将第一个正常数据包发送给一个默认网关。这个默认网关一般在操作系统中已经设好，对应第三层路由模块；所以对于不是同一子网的数据，最先在数据包中目的 MAC 地址中放入的是默认网关的 MAC 地址。然后由三层模块接收此数据包，查询路由表以确定到达 B 的路由。构造一个新的帧头，其中以默认网关的 MAC 地址为源 MAC 地址，以主机 B 的 MAC 地址为目的 MAC 地址。通过一定的识别触发机制，确立主机 A 与 B 的 MAC 地址及转发端口的对应关系，并记录进三层交换机流缓存条目表。以后的主机 A 到主机 B 的数据，就直接交由二层交换模块完成。这就是通常所说的一次路由，多次转发。

以上就是三层交换机工作过程的概括，从中可以看出三层交换具有以下的特点：

- 由硬件结合实现数据的高速转发。这不是简单的二层交换机和路由器的叠加，而是三层路由模块直接叠加在二层交换的高速背板总线上，突破了传统路由器的接

口速率限制。

- 简洁的路由软件使路由过程简化。大部分的数据转发，除了必要的路由选择交由路由软件处理外，都是由二层模块高速转发，路由软件大多都是经过处理的高效优化软件，并不是简单照搬路由器中的软件。

L3(三层)交换的实质是基于硬件的路由，数据包的发送也是通过 ASIC 芯片来完成的。其最重要的功能是加快大型局域网络内部数据的快速转发，加入路由功能也是为这个目的服务的。

3. L4 交换机功能和机制

L4(四层)交换技术可以简单的理解为交换机实现的一种特殊功能——数据流的负载均衡。它决定如何传输网络数据——不仅仅依据 MAC 地址(第二层地址)或源/目标 IP 地址(第三层地址)，而且依据 TCP/UDP(第四层)应用端口号。

第四层交换功能使用虚 IP 指向物理服务器。它传输的业务、承载的协议多种多样，有 HTTP、FTP、NFS、Telnet 或其他协议。这些业务在物理服务器基础上，需要用复杂的载量平衡算法进行数据流的分配。在 IP 世界，业务类型由终端 TCP 或 UDP 端口地址来决定；而在第四层交换中的应用区间，则由源端和终端 IP 地址、TCP 或 UDP 端口共同决定。

在四层交换中，交换机为每个提供服务的服务器组设立虚 IP 地址(VIP)，每组服务器支持某种应用。当某客户端进行应用请求时，一个带有目标服务器组的 VIP 连接请求(例如一个 TCP SYN 包)发给四层交换机。四层交换机则使用负载均衡的算法，然后在该后台服务器组中选取最好的服务器，并将客户端请求的目的 VIP 用实际服务器的 IP 取代，并将连接请求最终传给选取好的服务器。这样，同一区间的所有数据包由四层交换机进行映射，在用户和同一服务器间进行传输。

四层交换机通过以上的工作流程将网络数据流均衡到后台应用服务器组中的每台服务器上。下面将探讨其工作原理。

OSI 模型的第四层是传输层，负责端对端通信，即在网络源和目标系统之间协调通信。在 IP 协议栈中，传输层就是 TCP(传输控制协议)和 UDP(用户数据包协议)所在的协议层。

在第四层中，TCP 和 UDP 协议报头包含端口号(port number)，它们可以惟一区分每个数据包使用了哪些应用协议(例如 HTTP、FTP 等)。终端系统利用这种信息来区分包中的数据，尤其是端口号——使一个接收端计算机系统能够确定它所收到的 IP 包类型，并把它交给合适的高层软件。端口号和设备 IP 地址的组合通常称作“插口(socket)”。

对于 TCP/UDP 的端口号，1~255 之间的被保留，称为“保留”端口，除了“保留”端口外，标准 UNIX 服务分配在 256~1024 端口范围，定制的应用一般在 1024 以上分配端口号。

TCP/UDP 端口号提供的附加信息可以为网络交换机所利用。具有第四层交换功能的交换机能够起到与服务器相连接的“虚拟 IP”(VIP)前端的作用。

提供相关应用的服务器组所对应的每台服务器都映射到一个 VIP 地址。这个 VIP 地址被发送出去并在域名系统上注册。在客户端发出一个服务请求时，第四层交换机通过判定 TCP 或 UDP 以及其端口号来识别此次会话的开始。然后交换机利用复杂的均衡算法来确定处理这个请求的最佳服务器。一旦做出这种决定，交换机就将会话与一个具体的服务器 IP 地址联系在一起，并用该服务器真正的 IP 地址来代替该 VIP 地址。

四层交换机保存一个与被选择的服务器相配的源 IP 地址以及源 TCP 或 UDP 端口号相关联的连接表。然后四层交换机向这台服务器转发连接请求，所有后续包在客户机与服务器之间重新映射和转发，直到交换机发现会话终止为止。

4. 多层交换机功能和机制

光网络技术得到应用之后，随着网络容量的大幅提升，带宽已不再是关键问题，如何充分利用带宽资源对 Internet 上的应用、内容进行管理，日益成为服务提供商关注的焦点。在 GB 级带宽应用的情况下，网络层以下不再是问题的关键，取而代之的是提高网络服务水平，完成互联网向智能化的转变。

要解决区分应用、动态分配资源和用户计费等问题，用网络识别设备分发业务流量是一个很好的途径。在早期，当设备厂商开始关注这一问题的时候，提出的解决方案是通过专门的软件来实现内容识别功能，但在市场上并没有达到预期的效果。问题的关键在于完成上述功能所需的信息深埋在数据包的内部，而且只在网络会话建立时才出现一次。这就要求基于软件的内容识别设备窥视到会话的每个数据包的内部，结果就造成了严重的延迟和性能恶化，拥塞在所难免。

随后，全部用专用的特殊应用集成电路(ASIC 芯片)实现的多层交换技术开始在市场中出现。去掉了复杂的软件、通用 CPU 和网络处理器，通过应用交换机实现所有的网络功能，最大限度地利用网络资源。同时，多层交换把应用交换机放置在网络的核心层或者汇聚层，而不是紧靠下层的服务器，使网络管理者能够以更低的成本更好地分配网络资源成为可能。这种解决方案使服务提供商和企业用户可以不牺牲线速的千兆比特性能，而自由地设置网络应用和业务所要求的任何规则。

在当前的环境下，多层交换技术主要在于互联网和数据中心，比较成熟的产品大多为互联网服务的 Web 交换机。这些应用多层交换的设备在网络内容管理方面具有传统交换机的强大功能。在 Internet、企业内部网(Intranet)、企业外部网(Extranet)，多层交换机都有着广泛的应用。

在所有这些应用中，多层交换技术面向的不仅仅是当今的需求，更重要的是建立满足未来需求的可扩展分布式体系结构。这要求多层交换具有如下的特性：新的高可用性标准、通过 SSL 集成提高安全性和性能、本地和全球负载均衡、站点和系统安全性。

8.6.1.3 IP 路由器功能和控制

近几年来，基于 TCP/IP 协议的 Internet 已逐步发展成为当今世界上规模最大、拥有用户和资源最多的一个超大型计算机网络，TCP/IP 协议也因此成为事实上的工业标准。IP 网络正逐步成为当代乃至未来计算机网络的主流。路由器作为 IP 网络的核心设备，将不同的 IP 子网互联起来构成一个规模巨大的 IP 网络。

1. IP 路由器的功能

路由器是工作在 OSI 标准模型的第三层——网络层的数据包转发设备。路由器通过转发数据包来实现网络互联。虽然路由器可以支持多种协议(如 TCP/IP、IPX/SPX、Apple Talk 等协议)，但是在我国绝大多数路由器运行 TCP/IP 协议。路由器通常连接两个或多个由 IP 子网或点到点协议标识的逻辑端口，至少拥有 1 个物理端口。路由器根据收到数据包中的网络层地址以及路由器内部维护的路由表决定输出端口以及下一跳地址，并且重写链路层

数据包头，实现转发数据包。路由器通过动态维护路由表来反映当前的网络拓扑，并通过与网络上其他路由器交换路由和链路信息来维护路由表。

作为网络的核心设备，路由器应该具备以下功能：

(1) 接口功能　该功能用作将路由器连接到网络。路由器的接口可分为局域网接口和广域网接口两种。局域网接口主要包括以太网、令牌环、令牌总线、FDDI 等网络接口。广域网接口主要包括 E1/T1、E3/T3、DS3、通用串行口(可转换成 X.21 DTE/DCE、V.35 DTE/DCE、RS232 DTE/DCE、RS449 DTE/DCE、EIA530 DTE)等网络接口。

(2) 通信协议功能　该功能负责处理通信协议，可以包括 TCP/IP、PPP、X.25、帧中继等协议。

(3) 数据包转发功能　该功能主要负责按照路由表内容在各端口(包括逻辑端口)间转发数据包并且改写链路层数据包头信息。

(4) 路由信息维护功能　该功能负责运行路由协议并维护路由表。路由协议可包括 RIP、EIGRP、OSPF、ISIS、BGP 等协议。

(5) 管理控制功能　此功能可再细分为 SNMP 代理功能、Telnet(SSH)服务功能、本地管理、远端监控和 RMON(MIB)5 个功能。通过 5 种不同的途径对路由器进行控制管理，并且允许记录日志。

(6) 安全功能　该功能用于完成数据包过滤、地址转换、访问控制、数据加密、防火墙以及地址分配等。

2. IP 路由器的控制

路由器已经成为网络的关键。因此，对路由器做好配置就可以控制、调整网络中的数据流量，以达到我们的需求。下面将详细介绍路由器的配置、管理方法，考虑到 Cisco 路由器广泛的应用，在此将以 Cisco 路由器为例进行介绍。

(1) 基本配置方式

一般来说，Cisco 路由器有 5 种配置方式(如图 8.11 所示)：

- 使用路由器的 Console(控制台)接口，将配置线缆挂接到终端；或者挂接到运行终端仿真软件的微机。
- 使用 AUX(辅助)接口挂接 MODEM，通过电话线与远方的终端相连；或者将配置线缆挂接到运行终端仿真软件的微机。
- 通过网络中的 TFTP 服务器，上传、下载路由器的配置文件、路由器软件镜像等。
- 使用 Telnet 程序、远程配置管理路由器。
- 使用网络中的 SNMP 网管工作站管理路由器。

但是，对于出厂的路由器，第一次的设置必须通过第一种方式来进行。此时终端的硬件设置如下：

- 波特率　9600。
- 数据位　8。
- 停止位　1。
- 奇偶校验　无。

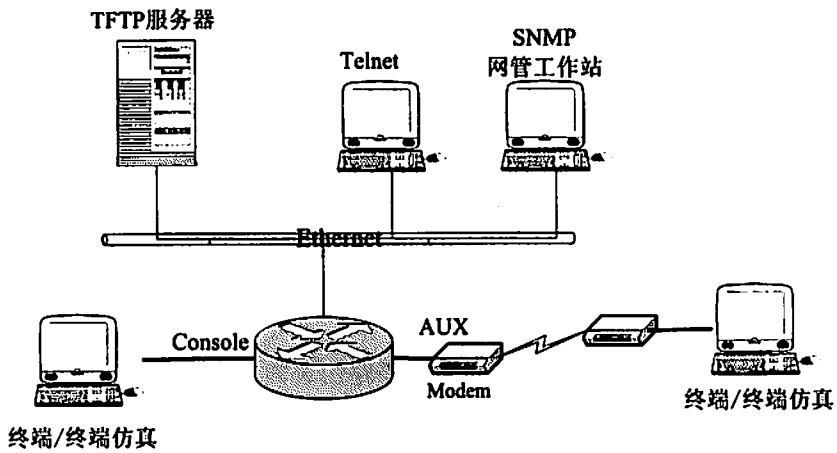


图 8.11 路由器的基本配置方式

(2) 用户命令模式

① router>

“>”符号表示路由器处于普通用户命令模式。此时用户可以查看路由器的连接状态，访问其他网络和主机等，但不能看到和更改路由器的配置内容。

② router#

“#”符号表示路由器处于特权用户命令模式。在普通用户模式“>”提示符下键入 enable 命令后，路由器即进入特权用户命令模式。这时不但可以执行所有的用户命令，还可以看到或者更改路由器的配置内容。

③ router(config)#

“(config)#”表示路由器进入了全局配置模式。在特权用户命令模式“#”提示符下键入 configure terminal，则可以进入此模式。此时，可以设置路由器的全局参数，如使能密码、静态路由、访问控制列表(ACL)等。

④ 其他命令模式

路由器还可能处在以下某个局部的配置模式下，此时可以设置路由器某个局部的参数。

a. router(config-if)#

在全局配置模式下，输入接口(interface)命令，进入此接口配置模式；此时，可以设置 IP 地址、封装模式等。

b. router(config-line)#

在全局配置模式下，输入线路(line)命令，进入此线路配置模式；此时，可以设置登录的模式、登录密码等。

c. router(config-router)#

在全局配置模式下，输入路由(router)命令，进入此路由配置模式；此时，可以设置路由宣告的网段、对等路由器(邻居)、路由再发布等。

⑤　“>”

“>”符号表示路由器处于 RXBOOT 状态，在开机后 60 秒内按 Ctrl+Break 可进入此状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导、密码修复等工作。

(3)　常用命令

①　帮助

在 Cisco 的网络操作系统(IOS)中，无论任何状态和位置，都可以键入“？”得到系统的帮助。

②　改变模式

改变模式的命令如表 8.2 所示。

表 8.2　改变模式的命令

任　务	命　令
进入特权配置模式	enable
退出特权配置模式	disable
进入对话配置模式	setup
进入全局配置模式	config terminal
退出全局配置模式	end
进入接口配置模式	interface *type slot/number*
进入子接口配置模式	interface *type number.subinterface* [point-to-point | multipoint]
进入线路配置模式	line *type slot/number*
进入路由配置模式	router *protocol*
退出局部配置模式	exit

③　显示(show)命令

显示命令如表 8.3 所示。

表 8.3　显示命令

任　务	命　令
查看版本及引导信息	show version
查看运行设置	show running-config
查看开机设置	show startup-config
显示接口信息	show interface *type slot/number*
显示路由信息	show ip router

④　拷贝(copy)命令

用于路由器镜像文件 IOS 及路由器配置文件的备份和升级：flash 存放 IOS 文件、config 为配置文件(命令的使用方法，详见图 8.12)。

⑤　网络命令

网络命令如表 8.4 所示。

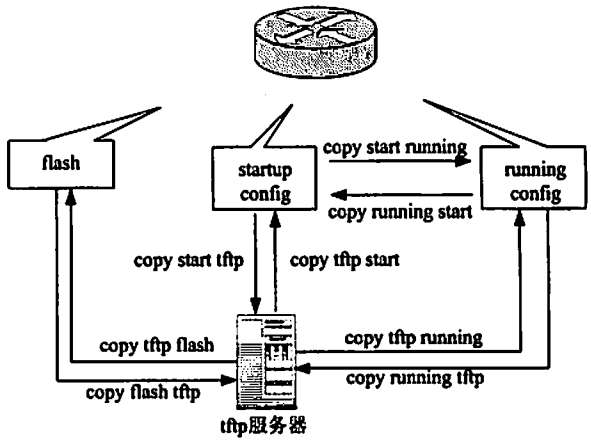


图 8.12 拷贝命令示意图

表 8.4 网络命令

任 务	命 令
登录远程主机	telnet *hostname* | IP address
网络侦测	ping *hostname* | IP address
路由跟踪	trace *hostname* | IP address

⑥ 基本设置命令

基本设置命令如表 8.5 所示。

表 8.5 基本设置命令

任 务	命 令
全局配置	config terminal
配置访问用户及密码	username *username* password *password*
配置特权密码	enable secret *password*
配置路由器名	hostname *name*
配置静态路由	ip route *destination subnet-mask next-hop*
启动 IP 路由	ip routing
启动 IPX 路由	ipx routing
接口设置	interface *type slot/number*
配置 IP 地址	ip address *address subnet-mask*
配置 IPX 网络	ipx network *network*
激活接口	no shutdown
物理线路设置	line *type number*
启动登录进程	login [local | tacacs server]
设置登录密码	password *password*

备注：命令行中的 *斜体字* 表示为相关的命令参数。

路由器的管理、配置非常注重动手实践，我们必须学而致用。在理论知识的引导下，经常进行配置练习，这样就可以熟能生巧。以上仅仅以 Cisco 路由器为范例介绍了基本的操作命令，这些是路由器管理的入门知识。若要深入学习，建议参考《Cisco 路由器配置手册》、《Cisco 路由器从入门到精通》等书籍。

3. 多协议路由器

如果按照对网络层协议的支持来作分类，路由器可分为单协议路由器和多协议路由器。单协议路由器只能实现具有相同网络层协议的网络互联；多协议路由器则可以实现具有不同的高层协议的网络的互联。

在实际应用中，要求进行互联的网络可能采用了不同的高层协议。比如，Novell 公司的 NetWare 的网络层与传输层协议分别为 IPX(Internetwork Packet Exchange)与 SPX (Sequential Packet Exchange)，通常记作 SPX/IPX。而 TCP/IP 协议作为实际上的工业标准被更多的网络所使用。

SPX/IPX 协议与 TCP/IP 协议有很多的不同之处。分布在 Internet 中的采用 TCP/IP 协议的主机只能通过 TCP/IP 的路由器与其他 Internet 中的 TCP/IP 主机进行通信，却不能与同一个局域网中或其他局域网中的采用 NetWare 协议的主机进行通信。同样，采用 NetWare 协议的主机也只能通过 NetWare 路由器与其他 Internet 中采用 NetWare 协议的主机进行通信，却不能与同一个局域网中或其他局域网中的采用 TCP/IP 协议的主机进行通信。可见，Internet 中主机之间的通信受到路由器所承载的高层协议的限制。

为了解决上述的通信问题，我们可以采用多协议路由器。多协议路由器具有处理多种不同协议分组的能力——它可以同时处理 IP 分组数据包和 IPX 分组数据包。同时，多协议路由器还具有对这两种不同类型的分组数据包进行路由选择，并完成分组数据包的转发功能。

多协议路由器同时要为不同类型的协议建立和维护不同的路由表——比如，IP 和 IPX 两种路由表，以便为不同分组数据包进行路径寻址、数据转发。

4. 路由协议

路由是把报文从一个网络转发到另一个网络的过程。路由是由源网络的设备——路由器根据特定路由协议的度量标准决定的，路由协议使用度量标准来决定到目的地的最好路径。度量标准有：路径长度、可靠程度、延迟、带宽、负载以及通信代价等。下面将介绍几种常用的路由协议：

- RIP(路由选择信息协议)　距离向量协议使用跳计数作为其尺度。RIP 协议广泛应用于路由选择业务，是内部网关协议(IGP)，它表示仅在一个自治系统(AS)内执行(自治系统是由同一行政单位管理的采用相同路由选择策略的网络)。RIP 协议最近的增强版是 RIP v2 规范，它允许 RIP 数据包携带更多的信息并提供简单认证机制。
- IGRP(内部网关路由选择协议)　Cisco 在 20 世纪 80 年代中期开发了此路由选择协议，从而为自治系统内的路由选择提供一个健壮的协议。IGRP 是一个距离向量内部网关协议。它使用度量的组合(向量)：时延、带宽、可靠性以及负载都是路由选择决策的要素。

- EIGRP(增强 Internet 网关路由选择协议) 该协议是对其前身 IGRP 的改进。EIGRP 是混合路由选择协议，它将链路状态协议与距离向量协议的性能相结合。EIGRP 综合了扩散更新算法(DUAL)。EIGRP 区别于其他路由选择协议的性能关键在于快速收敛，支持可变长子网掩码(VLSM)，支持部分更新以及多网络层协议(除了支持 IP，EIGRP 还支持 IPX 和 AppleTalk)。
- OSPF(开放最短路径优先) 链路状态路由选择协议，它要求向同一等级区域中所有路由器发送链路状态公告(LSA)。OSPF 的 LSA 包括所附接口、所用度量及其他变量信息。OSPF 路由器收集链路状态信息时，使用最短路优先(SPF)算法计算到每个节点的最短路径。与 RIP 不同，OSPF 可在分级网中运行。分级网中最大的实体是自治系统。尽管能够从其他自治系统接收路由信息或发送路由信息到其他自治系统，OSPF 还是一个内部网关路由选择协议。自制系统可分为许多区域，它们是相邻网络及所连主机的集合。
- BGP(外部网关协议) 该协议用来在多个自治系统或域间实现路由选择，并与其他 BGP 系统交换路由选择和可到达性信息。BGP 被开发以取代现已过时的旧版本 EGP，作为标准外部网关路由选择协议在全球因特网中使用。BGP 克服了 EGP 的严重缺陷，且更好地适应了 Internet 的发展。

8.6.2 典型例题分析

例 1 下面是某路由器的配置信息，解释_____处有下划线部分的含义。(2004 年上半年下午试题四)

配置路由器信息：

```
Current configuration:
!
Version 11.3
no service password-encryption
!
hostname Router1                                    第__(1)__处
!
enable password pwd12345                            第__(2)__处
!
interface Ethernet0
ip address 192.4.1.1 255.255.255.0
!
interface Serial0
ip address 192.3.1.1 255.255.255.0
encapsulation frame-relay IETF                      第__(3)__处
no ip mroute-cache
bandwidth 2000                                      第__(4)__处
frame-relay map ip 192.3.1.2 100 broadcast          第__(5)__处
frame-relay lmi-type cisco
!
router ospf 1                                       第__(6)__处
```

```
network 192.1.1.0 0.0.0.255 area 0          第__(7)__处
network 192.3.1.0 0.0.0.255 area 0
network 192.4.1.0 0.0.0.255 area 0
neighbor 192.1.1.2                          第__(8)__处
!
End
```

分析：从路由器控制小结中，我们得知关于 CISCO 路由器的配置方法以及相关命令。对于(1)处的命令是“hostname Router1”，从而知道这是路由器的命名命令，该路由器名为 Router1。对于 OSPF 路由协议，其在 CISCO 路由器的实现有别于其他路由协议。比如，OSPF 采用的是子网通配符而不是子网掩码，也叫做“子网掩码的反码”，其计算公式为：

子网通配符=255.255.255.255-子网掩码

同时，OSPF 使用多区域(area)的层次区域拓扑结构。这种配置方法带来的优点是：减少了 CPU 开销(这些开销是由于频繁地进行最短路径优先(SPF)计算而引起的)；路由表维持最小的规模；(路由汇总极小化 LSU 的开销)，从而保护了带宽。ID 为 0 的区域也叫做骨干区域，主要用来进行交互 OSPF 非骨干区域的路由信息。

答案：

(1) 路由器名为 Router1。

(2) 特权(使能)密码为 pwdl2345。

(3) 在串口“Serial0”配置中封装帧中继，并且帧中继数据包封装格式为 IETF。

(4) 限定串口“Serial0”的带宽为 2M。

(5) 将 IP 地址与帧中继地址进行映射。对端路由器接口的 IP 地址为 192.3.1.2，而本端口的帧中继号码为 100，并且使用广播方式在帧中继线路上传送路由信息。

(6) 在路由器上启动 OSPF 动态路由协议，并且该 OSPF 路由进程 ID 为 1。

(7) 指定与该路由器相连的网络 IP 为 192.1.1.0，子网通配符为 0.0.0.255，网络区域 ID 为 0。

(8) 指定与该路由器相邻的路由器的 RouterID 为 192.1.1.2。

例 2　阅读以下说明，给出_____处的解答。(2003 年下午试题五)

【说明】

某网络结构如图 8.13 所示，如果 Router3 与网络 4 之间的线路突然中断，按照 RIP 路由协议的实现方法，路由表的更新时间间隔为 30 秒，中断 30 秒后 Router2 的路由信息表 8.6 和中断 500 秒后 Router2 的路由信息表 8.7 如下。

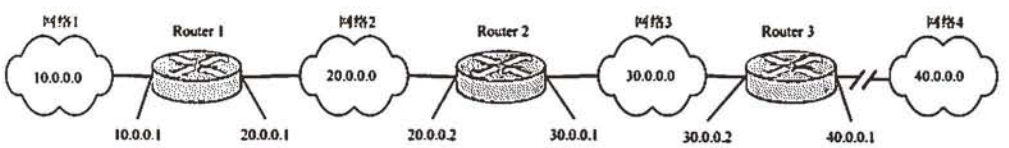


图 8.13　网络拓扑图

注：

(1) 若到达目的网络不需转发或目的网络不可达，用“—”来表示“下一站地址”。

(2) 当目的网络不可达时，“跳数”为 16。

表 8.6 路由信息表 1

目的网络	下一站地址	跳数
10.0.0.0	(1)	(2)
20.0.0.0	—	0
30.0.0.0	—	0
40.0.0.0	(3)	(4)

表 8.7 路由信息表 2

目的网络	下一站地址	跳数
10.0.0.0	20.0.0.1	1
20.0.0.0	(5)	(6)
30.0.0.0	(7)	(8)
40.0.0.0	(9)	(10)

【问题】

1. 请填充中断 30 秒后 Router2 的路由信息表 1。
2. 请填充中断 500 秒后 Router2 的路由信息表 2。

分析：RIP 使用广播用户数据报协议(UDP)的数据报文方式，把路由表项发送到相邻路由器。因为 RIP 使用 UDP 作为其发送机制，所以发送到相邻路由器的路由表更新不能得到保证。而路由器间 RIP 表项的发送缺省是在路由器初始启动后 30 秒(周期性更新)。当一个路由器在到另一个已经活动的路由器的连接上变成活动时，这种路由器的“公布”也会出现在路由器之间。

使用 RIP 的路由器，期待在 180 秒(6 个更新周期)之内从邻接路由器获得更新。如果在这段时间内没有收到邻接路由器的路由表更新，则去往未更新路由器的网络路由被标识为不可用，强制把 ICMP 网络不可到达消息返回给通过未更新路由器而连接的资源请求者。一旦接收更新计时器到达 240 秒(8 个更新周期)，未更新路由器的路由表项将被从路由表中移去。

根据图 8.13 所体现的网络拓扑，在路由器 Router3 与网络 4 之间的线路突然中断之后，在第一个更新周期(30 秒)之后和 180 秒之前路由器 Router 2 的路由表信息如同没有中断一样。而在 500 秒之后，由于路由器 Router 2(在 240 秒内)一直得不到关于网络 4 路由更新，因此网络 4 被从路由表中移去——不可达。

答案：

1. (1)20.0.0.1 (2)1 (3)30.0.0.2 (4)3
2. (5)- (6)0 (7)- (8)0 (9)- (10)16

8.6.3 同步练习

1. 简述中继器、交换机和路由器功能特点的差别。

2. RIP 是基于__(1)__的路由协议，此类路由协议的最优路径选择是由一个报文到达目的地之前必须经过的跳跃数(路由设备数)而决定的。EIGRP 和 IGRP 用同样的度量标准，这些值是__(2)__、__(3)__、__(4)__和__(5)__。这种标准用于 EIGRP 路由的缺省值是每一跳跃的最小带宽加上每一跳跃的特殊介质延迟。OSPF 是一种__(6)__IP 路由协议。OSPF 能够适应大型全局 IP 网络的扩展，而基于__(1)__的 IP 路由协议如 RIP 和 IGRP 则不能适应这种网络。OSPF 路由器具有惟一的标识符，称为__(7)__。

3. 如果互联的局域网采用了两种不同的网络层协议，则需要使用_____来连接。

8.6.4 同步练习参考答案

1. 略。
2. (1)距离向量　(2)带宽　(3)延迟　(4)可靠性　(5)负载
   (6)链路状态　(7)路由器 ID
3. 多协议路由器

8.7 本 章 小 结

本章主要要求考生掌握如何将 LAN 和 WAN 进行互联，互联所需要使用到传输技术、网络设备及操作、无线技术以及安全防护。主要内容包括了当前宽带的接入技术(ISDN、xDSL)、帧中继(FR)和 ATM 的传输技术、VPN 和远程访问服务以及网络互联设备的操作等基础知识。

第 9 章　网络应用服务

大纲要求：

- 地址服务　机制、DHCP、IPv6(机制和传输技术)。
- DNS(功能、机制)　域名、FQDN。
- 电子邮件(功能、机制)　SMTP、POP、MIME、IMAP、LDAP、邮件列表、Web Mail。
- 电子新闻(功能和机制、NNTP)。
- Web 服务(功能和机制、HTTP)。
- 负载分布(Web 交换)。
- 电子身份验证(功能、机制、认证授权、电子证书)。
- 服务机制　服务供应商、供应商漫游服务、拨号 IP 连接、CATV 连接、IP 电话、因特网广播和组播、电子商务、电子政务、移动通信、EZweb、主机服务提供者、EDI(规则、表单、Web EDI)、B2B、B2C、ASP、数据中心。

9.1　地 址 服 务

9.1.1　考点辅导

9.1.1.1　IP 地址的分类

IP 地址格式使用的是点分十进制表示法。它包含 32 位，分为四个部分，每个部分都是 8 位二进制字节的十进制表示。一个 IP 地址的二进制 8 位字节格式如：10000001.00000101.00001010.01100100，转换为十进制就是 129.5.10.100。地址的一部分是网络标识符(Net_ID，网络 ID)，另一部分是主机标识符(Host_ID，主机 ID)。

IP 地址共有 5 类，A 类、B 类、C 类、D 类和 E 类。在不同类型的网络中使用不同的 IP 地址类。地址分类反映了网络的大小以及包是单点传送的，还是多点传送的。

A 类、B 类和 C 类地址计划用于单点编址方法，但每一类代表着不同的网络大小。A 类地址用于最大型的网络，该网络的节点数可达 16 777 216 个，在最前 8 位(第一字节)上由 1~126 之间的值来标识。网络 ID 为前 8 位(第一字节)，主机 ID 为后 24 位(第三字节)。B 类地址是用于中型网络的单点编址格式，节点数可达 65 536 个，在最前 8 位(第一字节)上由 128~191 之间的值来标识；前两个 8 位(第一、二字节)为网络 ID，后两个 8 位(第三、四字节)是主机 ID。C 类地址是用于 256 个节点以下的小型网络的单点网络通信；最前面的 8 位(第一字节)转换为十进制是在 192~223 之间，网络 ID 为前 24 位(第一、二、三字节)，而主机 ID 为最后 8 位(第四字节)。

D 类地址并不反映网络的大小，只反映了通信是多点传送的，通常也称为组播。4 个 8 位字节用来指定所分配的接收多点传送的节点组，这个节点组由多点传送订阅成员组成。

D 类地址的范围为 224.0.0.0~239.255.255.255。

E 类地址用于试验，地址的第一个 8 位字节的范围为 240~255。

除了这些用于分类编址的 IP 地址外，还有一些特殊目的的 IP 地址，如 255.255.255.255，这是发送到所有网络位置的广播地址。以 127 作为第 1 个 8 位字节开始的数据包用于网络测试。对于一个完整的网络，只需提供网络 ID 号，其他字节均为 0 便可指定。例如：B 类地址网络 132.155.0.0，C 类地址网络 220.127.10.0。

根据用途和安全性级别的不同，还可以将 IP 地址分为两类：公共地址和私有地址。公共地址在 Internet 中使用，可以在 Internet 中随意访问。私有地址只能在内部网络中使用，只有通过代理服务器才能与 Internet 通信。

一个机构或网络要连入 Internet，必须申请公共 IP 地址。但是考虑到网络安全和内部实验等特殊情况，在 IP 地址中专门保留了三个区域作为私有地址，其地址范围如下：

10.0.0.0/8：10.0.0.0~10.255.255.255

172.16.0.0/12：172.16.0.0~172.31.255.255

192.168.0.0/16：192.168.0.0~192.168.255.255

使用保留地址的网络只能在内部进行通信，而不能与其他网络互联。因为本网络中的保留地址同样也可能被其他网络使用，如果进行网络互联，那么寻找路由时就会因为地址的不惟一而出现问题。但是这些使用保留地址的网络可以通过将本网络内的保留地址转换成公共地址的方式实现与外部网络的互联，这里需要使用网络地址转换技术。

9.1.1.2 子网掩码

编址的另一个特殊的形式是子网掩码。子网掩码的目的有两个：一是显示使用的编址类别；二是将网络分成子网来控制网络流量。在第一种情况下，子网掩码可使得应用程序能够确定 IP 地址的哪一部分是表示网络 ID，哪一部分是表示主机 ID。例如，一个 A 类地址网络的默认子网掩码是第一个 8 位字节中均为二进制的 1，其他均为二进制的 0：11111111.00000000.00000000.00000000(255.0.0.0)。

要将网络分成子网，子网掩码应包含子网 ID，这个子网 ID 是由网络管理员决定的，存在于网络 ID 和主机 ID 之内。例如，可以指定 B 类地址的整个第三个 8 位字节来说明子网 ID，如 11111111.11111111.11111111.00000000(255.255.255.0)。另一种选择是只指定第 3 个 8 位字节的前 5 位作为子网 ID，最后 3 位和余下的 8 位字节用于指定主机 ID，如 11111111.11111111.11111000.00000000(255.255.248.0)。

使用子网掩码将网络分成一系列小型网络，使得第 3 层设备可以有效地忽略传统的地址分类命名，因此通过多个子网和额外的网络地址将网络分段时就有了更多的选项，克服了 4 个 8 位字节长度的限制。同样是利用子网掩码工具，1992 年出现了一种新的忽略地址分类命名的方法，它是 CIDR(Classlees Interdomain Routing，无分类域间路由)编址方法。

引入 CIDR 后，意味着网络“类”(比如：A 类地址、B 类地址等)的概念已经被取消，取而代之是“网络前缀”的概念。CIDR 的基本思想是取消地址的分类结构，允许以可变长分界的方式分配网络数。它支持路由聚合，可限制 Internet 主干路由器中必要路由信息的增长。

CIDR 编址的方法是在点分隔的十进制符号之后画一个斜杠“/”，再加上子网掩码“1”的总个数。比如：202.102.0.0/23；我们知道，202.102.0.0 是 C 类网络地址(默认是 24 位子网掩码)；而采用这样的 CIDR 编址后，202.102.0.0/23(23 位子网掩码)不属于 C 类网络地址也不属于 B 类网络地址。但是，202.102.0.0/23 网络地址提供了更多的信息节点(510 个)，而默认的 202.102.0.0 C 类网络地址只提供 254 个信息节点。

可见，CIDR 编址方法为中型的网络提供了更多的 IP 地址选项。例如，对于需要 262 144 个节点的网络，其 CIDR 网络编址方案可以是 165.100.0.0/14。

9.1.1.3 DHCP

DHCP 全名是主机动态配置协议(Dynamic Host Configuration Protocol)，它是 BOOTP 的扩展，是基于 C/S 模式的。DHCP 主要用于大型网络环境和配置比较困难的地方，其主要功能是让一台主机能够通过自己的以太广播，从 DHCP 服务器处获得相关的网络参数，如网络地址、子网掩码、默认网关、DNS 服务器地址等。

DHCP 可以实现 IP 地址的租用。对于拥有许多台计算机的大型网络来说，每台计算机拥有一个 IP 地址有时候可能是不必要的或是浪费的，因此租用 IP 地址是一种更好的解决办法。IP 地址的租期可以从 1 分钟到 100 年不定，当租期到了的时候，服务器可以把这个 IP 地址分配给别的机器使用。客户也可以请求使用自己喜欢的网络地址及相应的配置参数。

同时，DHCP 继承了 BOOTP 的包格式：这样它也就可以使用 BOOTP 的转发代理来发送 DHCP 包了，这使得 BOOTP 和 DHCP 之间可以实现互操作。对于 BOOTP 转发代理来说，发的是 DHCP 包还是 BOOTP 包，它根本不需要了解，其使用的服务器端口号是 67 和 68。DHCP 在以下几个方面对 BOOTP 进行了扩展：

- DHCP 定义了一种可以使 IP 地址使用一段有限时间的机制，在客户期限到了的时候可以重新分配这个 IP 地址。
- DHCP 为用户提供所有 IP 配置参数。
- DHCP 包长度比 BOOTP 包长度稍长，多出的长度里包括了网络配置参数。
- DHCP 有七种消息类型，而 BOOTP 只有两种。

客户机请求获得网络地址和配置参数的最初几个步骤为：

(1) 客户机首先发出请求数据包，名称叫 DHCP-DISCOVER(而服务器返回包的名称叫 DHCP-OFFER)。

(2) BOOTP 转发代理接收到请求包，并负责向其网络内的 DHCP 服务器转发。

(3) DHCP 服务器以 DHCP-OFFER 包响应客户的要求，这个包内包括可用的 IP 地址和参数。

(4) BOOTP 转发代理接收到 DHCP-OFFER 包，并对它进行检查。如果它觉得没有问题，就向客户转发。

(5) 客户机可以同时接收到多个服务器的应答，它可以自己决定用哪一个。

在客户机决定了使用某个服务器以后，其向服务器发送应答时的情况如下：

(1) 当客户选定了某个目标服务器后，它会广播 DHCP-REQUEST 包，用以通知选定的服务器和未选定的服务器。

(2) 转发工作仍然由 BOOTP 转发代理担任。

(3) 收到 DHCP-REQUEST 包的服务器会检查收到的包，如果包内的地址和提供的地址一致，证明现在客户机选择的是这台服务器提供的地址；如果不是，表明自己提供的地址被拒绝。

(4) 被选定的服务器在接收到 DHCP-REQUEST 包以后，因为某些原因可能不能向客户提供这个网络地址或参数，它会向客户发送 DHCP-NAK 包；如果可以提供网络地址或参数，则会向客户发送 DHCP-ACK 包。

(5) 客户机在收到包之后，检查内部的网络地址和租用时间，如果客户机觉得这个包有问题，它可以发送 DHCP-DECLINE 包拒绝这个地址，然后重新发送 DHCP-DISCOVER 包。如果觉得没有问题，则接受这个配置参数。如果，客户机接收到的是 DHCP-NAK 包时，它将重新发送 DHCP-DISCOVER 包。

客户机在 IP 地址租期快结束时(用户下一次可以再次获得相同的 IP 地址)，DHCP 更新的具体实现步骤为：

(1) 客户机在发送的 DHCP-REQUEST 包(可由 BOOTP 转发代理转发)内包括自己以前使用的 IP 地址。

(2) DHCP 服务器检查 DHCP-REQUEST 包内包括的配置参数。

(3) 如果该 DHCP 服务器是原来提供这个网络地址参数的服务器，它会以 DHCP-ACK 包回应。

(4) 客户机接收到 DHCP-ACK 包后，可以接收或拒绝；如果拒绝，可以重新申请新的网络地址。

(5) 如果服务器觉得客户机的请求是无效的，服务器会以 DHCP-NAK 包响应，客户机接收到这个数据包后，为了重新获得网络地址会再次发送 DHCP-DISCOVER 包。

9.1.1.4 IPv6

到目前为止 IPv4 已经存在 20 多个年头了。在 20 世纪 90 年代中期，人们就认识到了它的局限性，主要的一点是 32 位地址太有限。在当前的网络使用状况下，IPv4 所有的地址很快将会消耗尽。

另外，由于 IPv4 不能提供网络安全，也不能实施复杂的路由选项(如在 QoS 的水平上创建子网等)，所以应用也受到了限制。同时，IPv4 除了提供广播和多点传送编址外，并不具备多个选项来处理多种不同的多媒体应用程序(如流式视频或视频会议等)。

为适应 IP 的爆炸式应用，Internet 工程任务组(IETF)开始了 IPng(IP next generation)的初步开发。1996 年，IPng 的研究诞生了一种称为 IPv6 的新标准，并在 RFC 1883 中得到定义。IPv6 的目的是从 IPv4 中提供一条逻辑的增长路径，使得应用程序和网络设备可以处理新出现的要求。目前，IPv4 仍应用在全世界的绝大多数网络中，但向 IPv6 的升级已经开始了。IPv6 的新特点有：

- 128 位编址能力。
- 一个单独的地址对应着多个接口。
- 地址自动配置和 CIDR 编址。

- 40 个字节的头取代了 IPv4 的 20 个字节的头。
- 可将新的 IP 扩展的头用于特殊需要，包括用于更多的路由技术和安全选项中。

IPv6 编址使得一个 IP 标识符可以与多个不同的接口相关，从而可以更好地处理多媒体信息流量。在 IPv6 网络中，传送的多媒体流量不是进行广播或多点传送，而是将所有接收接口都指定为同一个地址。

IPv6 并不沿基于分类的地址而行，而是与 CIDR 兼容的，从而地址可以通过很大范围的选项来进行配置，并使得路由和子网的通信更出色。同时，它还提供了选项，使得我们可以在一个组织内、一个单独的地址内，根据地理位置、组织及其类型等来创建各异的网络。IPv6 编址是自动配置的，可以减轻网络管理员管理和配置地址的工作负荷。它支持两种自动配置技术：一种是基于动态主机配置协议(DHCP)；另一种自动配置技术是无状态的。在无状态自动配置中，网络设备指派自己的 IP 地址，而不是从服务器中获得。它简单地通过将 NIC 的 MAC 地址与从子网路由器中获得的子网命名结合在一起来创建地址。

IPv6 数据包的传送类型分为：单点传送、任意点传送和多点传送。在单点传送包中，一个单独的网卡接口对应一个单独的地址，并且是点到点传输的。任意点传送的包中包含着一个与多个接口关联的目标地址，而且这些接口通常是位于不同的节点上。任意点传送的包只向最近的接口传送，并不试图到达具有同一地址的其他接口。多点传送包与任意点传送包相似，具有与多个接口相关联的目标地址，但是与任意点传送包不同的是多点传送包将流向具有这个地址的所有接口。

1. 头部格式

基本的 IPv6 头包含以下域(如图 9.1 所示)：

- 版本：这是版本标识符，值为 6。
- 流量分类：该域说明了一个包是否包含着协助控制网络阻塞的信息。用于阻塞控制的包可以提供诸如过滤、自动 E-mail 投递和与 Internet 相关的控制等特征。不控制阻塞的包是携带数据的，可以指定不同的优先级来说明丢弃一个包对信息的影响。例如，携带声频的包的优先级应当设置得高一些，说明一定要避免丢弃包，因为这样会干扰声音播放的连续性。
- 流标签：此处的信息用于向路由器说明包需要以特殊的方法来进行处理。例如，多点传送包需要额外的网络资源，而秘密的包需要更高的安全性。
- 有效负载长度：该域说明了包有效负载的大小(不计包的头)。
- 下一个头：由于可以添加扩展的头，所以在基本的头到了结尾时，该域就提供了有关预期的头是何种类型的信息。如果没有包含扩展的头，那么下一个头就是 TCP 或者 UDP。
- 跳数限制：对 IPv4 TTL 域的修正。当创建好一个包后，就会在跳数限制(Hop Limit)域中输入最大的路由器跳数值，每次包经过第 3 层设备时，该值都会减 1。当第 3 层设备遇到的包的跳数限制为 0 时，就将该包丢弃，以免在网络上不断地传播。
- 源地址：这是发送设备的 128 位的地址。
- 目标地址：此域包含着接收包的设备的 128 位地址。

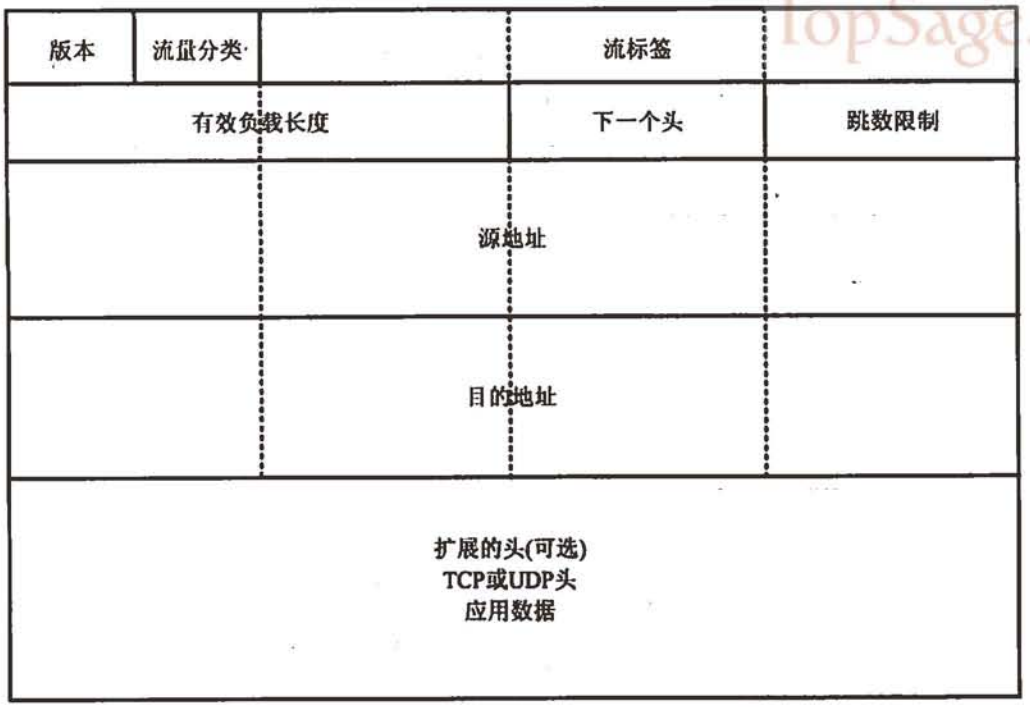


图 9.1　IPv6 数据包

2. IPv6 扩展头部及其功能

当前，IPv6 定义了 6 种扩展头，分别是：

- 步跳扩展头
- 路由扩展头
- 分段扩展头
- 验证扩展头
- 安全负载封装扩展头
- 目标选项扩展头

IPv6 的主头必须出现在所有的扩展头之前。扩展头是可选的，可以组合使用，也可以一个都不用。在单个的包中，每种类型的扩展头只能出现一次。当同时使用多个扩展头时，它们必须严格遵守上面列举的顺序。例如，如果同时使用了路由扩展头、验证扩展头和安全负载封装扩展头，那么包头的域必须按照如下的顺序出现：①IPv6 的主头；②路由扩展头；③验证扩展头；④安全负载封装扩展头；⑤TCP 或 UDP 头；⑥应用数据，如图 9.2 所示。在每一个扩展头中，第一个字节为一个 8 位的“下一个头(Next Header)”字段，该字段用以指明后面紧跟的是哪个头。在最后一个扩展头中，“下一个头”域包含的值为 59，表明该扩展头是最后一个。在上面的例子里，路由扩展头中的“下一个头”域指出后面紧跟的是验证扩展头；验证扩展头的“下一个头”域指出后面紧跟的是安全负载封装扩展头。除分段扩展头之外，在“下一个头”域之后紧跟着的是一个 8 位的“头扩展长度”域，用于指明该扩展头的长度。每个扩展头的长度必须为 8 的倍数个字节。

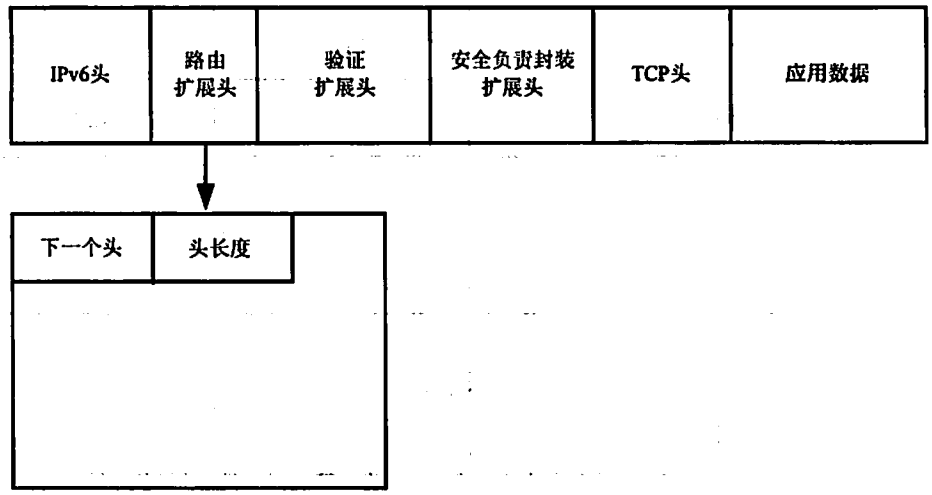


图 9.2 IPv6 数据包扩展头

步跳扩展头用于大数据的传输，例如：多媒体视频数据包。其应用数据负载可以从 65535 个字节到 4 亿个字节。数据包所经过的每一个路由都将读取步跳扩展头，这样会略微增加路由器的处理延迟。

路由扩展头使用按顺序排列的路由地址来标识整个路由，用户可以通过配置该头达到让包沿相同路径传输的目的，这种包可用于某些特殊的情况，例如：当某条路径上的路由器出现故障的时候。

在 IPv6 中，每个发送节点通过使用搜索包，运行一个路径最大传输单元(MTU)发现的过程，便可以确定接收网络所允许的最大包尺寸。该路径发现产生的信息包括是否有某个路由器出现故障和目标网络是否需要较小的包(IPv6 包最多可以包括 1280 个 8 位字节)。当向使用小于 1280 个 8 位字节包的网络上发送包时，IPv6 便对包进行分段。根据 MTU 路径发现所获取的信息，发送节点将数据包进行分段，在包头中添加分段扩展头，告知接收者包是如何分段的。将数据包分段的能力在从以太网向令牌环网发送包或者在具有不同包大小的快速以太网和千兆以太网之间传输数据时尤为重要。当把一个包进行分段后，每一个段都分配一个分段组内的标识符(每组是惟一的)；该标识符放入 32 位标识符域，这样在接收数据的时候，不同组的分段就可以很容易地区分开。

验证扩展头可用于确认数据包的完整性(IP 头、TCP 头、数据)，即保证接收到的数据包和发送的数据是一致的。每一个扩展头的每一个域以及负载数据都需要进行验证。如果在数据包发出后某个域中的值有所改动(对于步跳计数来说肯定要发生变化，因此步跳计数除外)，该字域的验证值则为 0。通常，验证扩展头和安全负载封装扩展头是一起使用的，这样便可以对包进行验证和加密/解密。当使用这两个扩展头时，在接收节点上将做如下处理：

(1) 首先验证 IP 头，然后验证 TCP 头(如果 IP 头或者 TCP 头被加密，则首先需要进行解密)。

(2) 在验证之后，使用安全负载封装扩展头中的信息对负载进行解密。

(3) 在解密了负载后，对负载进行验证。

在有安全需求的网络上，可以使用安全负载封装扩展头对 IP 包负载或者 TCP/IP 头和负载进行加密，该扩展头支持与数据加密标准(DES)相兼容的密钥加密技术。

9.1.2　典型例题分析

例　阅读以下说明，回答问题(1)~问题(4)。(2002 年下午试题一)

【说明】

设有 A，B，C，D 4 台主机都处在同一个物理网络中，A 主机的 IP 地址是 192.155.12.112，B 主机的 IP 地址是 192.155.12.120，C 主机的 IP 地址是 192.155.12.16，D 主机的 IP 地址是 192.155.12.222。共同的子网掩码是 255.255.255.224。

【问题】

1. A，B，C，D 4 台主机之间哪些可以直接通信？哪些需要通过设置网关(或路由器)才能通信？请画出网络连接示意图，并注明各个主机的子网地址和主机地址。

2. 若要加入第 5 台主机 E，使它能与 D 直接通信，其 IP 地址的设定范围应是多少？

3. 不改变 A 主机的物理位置，将其 IP 改为 192.155.12.168，试问它的直接广播地址和本地广播地址各是多少？若使用本地广播地址发送信息，请问哪些主机能够收到？

4. 若要使主机 A，B，C，D 在这个网上都能够直接通信，可采用什么办法？

分析：知道四台主机的 IP 以及子网掩码，我们可以算出其各自所在的网络：只要将 IP 地址与子网掩码进行逻辑“相与”运算，即可获得。

A 的 IP 地址 192.155.12.112 与 255.255.255.224 进行“相与”运算得到的结果为：192.155.12.96，则主机 A 是属于网段 192.155.12.96/27 的。同理得到，B 主机属于网段 192.155.12.96/27，C 主机属于网段 192.155.12.0/27，D 主机属于网段 192.155.12.192/27。

对于新加入的主机 E，要能与主机 D 直接通信，则它们应该同属于一个网段 192.155.12.192/27。因此，主机 E 可用的 IP 地址范围为：192.155.12.193~192.155.12.221。

如果主机 A 的 IP 改为 192.155.12.168 话，则其所在的网段为：192.155.12.160/27，因此它的直接广播地址是 192.155.12.191，本地广播地址是 255.255.255.255。我们知道，路由器的其中功能是隔断广播域，也就是阻断本地广播；所以，主机 A 使用本地广播地址发送信息，则只有在同一物理网段内的主机 B 可以接收到。

如果要使得主机间可以直接进行通信的话，则它们应该都同属于同一个网段。而当前四台主机 A，B，C，D 的 IP 地址都是属于 C 类 IP 地址 192.155.12.0/24 进行子网划分后的网段内的。因此，只要将这些子网网段重新聚合成为 C 类网段，它们就可以重新回归到网段 192.155.12.0/24；方法就是修改它们的子网掩码。

答案：

1. A、B 两台主机之间可以直接通信。A、B 与 C 之间通过路由器方能通信。A、B 与 D 之间通过路由器方能通信。C 与 D 之间通过路由器方能通信。示意图如图 9.3 所示。

2. IP 地址的范围是：192.155.12.193~192.155.12.221。

3. 直接广播地址是 192.155.12.191；本地广播地址是 255.255.255.255；若使用本地广播地址 255.255.255.255 发送信息，则 B 主机可以接收。

4. 将子网掩码改为 255.255.255.0(即 C 类地址的默认子网掩码)。

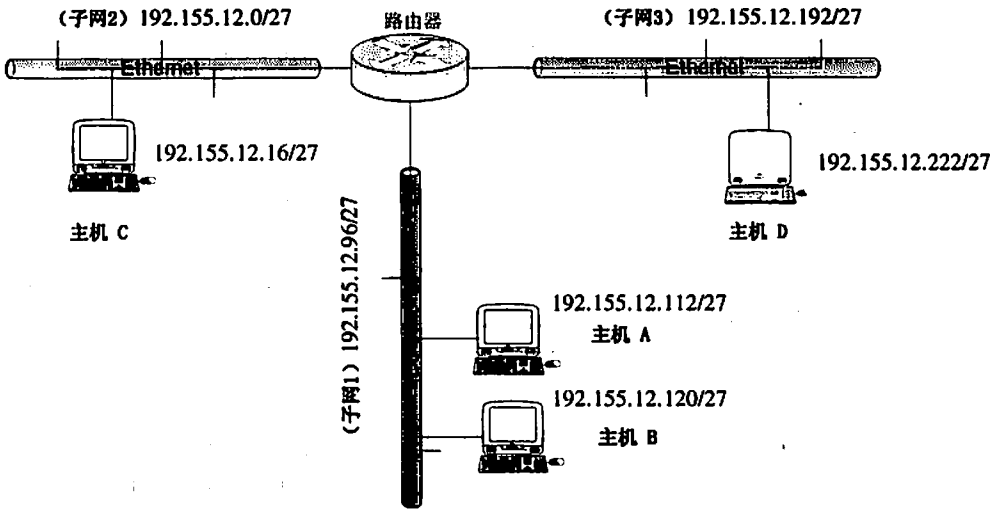


图 9.3 局域网示意图

9.1.3 同步练习

1. IP v6 将 IP 地址空间从__(1)__位扩展到__(2)__位。

2. 子网掩码为 255.255.255.0 代表什么意义。

3. 单位分配到一个 B 类的 IP 地址，其 Net-ID 为 172.250.0.0。该单位有 4 000 台机器，分布在 16 个不同的地点。请分析：(1)选用子网掩码为 255.255.255.0 是否适合；(2)给每一个地点分配一个子网号码，算出每个主机号码的最小值和最大值。

9.1.4 同步练习参考答案

1. (1)32 (2)128

2. 若是 A 类网络的子网掩码，则前 8 位为网络号，中间 16 位为子网号，最后 8 位为主机号；若是 B 类网络，则前 16 位为网络号，中间 8 位为子网号，最后 8 位为主机号；若是 C 类网络，则为 C 类网络的默认子网掩码。

3. (1)选用子网掩码为 255.255.255.0，子网位有 8 位，每个子网最多有 254 台主机(2^8-2=254)。如果 4000 台机器是平均分配的，则 4000÷16=250 台——不超过 254 台，选用这个子网掩码是合适的；如果不是平均分配，当某个子网主机数目超过了 254 台，选用这个子网掩码是不合适的。(2)如果还是选用 255.255.255.0 作为子网掩码，每个子网中主机号为 0.0.0.1～0.0.0.254。

9.2 应用层服务

TCP/IP 应用层支持多种协议，以便使各种应用能够工作。这些应用服务包括电子邮件、终端仿真、文件传输、路由、网络管理等。最常使用的应用服务是 DNS 域名系统、电子邮

件、电子新闻和 Web 服务。

9.2.1 考点辅导

9.2.1.1 域名系统

通常情况下，Internet 上的主机系统使用 IP 地址来标识。虽然使用 IP 地址对于网络和路由器很方便，但是用户还是更容易记住主机系统的名称。使用名称而不仅仅是 IP 地址，用户能更精确地记住，系统管理员也可以随意移动系统、更改 IP 地址，而不需要事先告诉用户新的 IP 地址。

域名系统(Domain Name System，DNS)是一种用于 TCP/IP 应用程序的分布式数据库，它提供主机名称和 IP 地址之间的映射、转换。DNS 使得主机能够根据名称获得对应的 IP 地址或通过 IP 地址获得对应的主机名称。

1. 域名

从概念上来说，Internet 被分成 200 多个顶级域(domain)，每个域包含许多主机。每个域又被分成若干个子域，子域又被进一步划分，以此类推。

顶级域有两种：通用域和国家域。常见的通用顶级域有：.com(商业机构)、.edu(教育网站，一般是学院和大学)、.gov(政府机关)、.org(非营利机构)、.net(网络运营机构)、.biz(商业机构)和.coop(合作机构)等。每个国家都有一个国家域，其定义位于 ISO 3166 中。

域名服务器的数据库形成一个倒立的树状结构，如图 9.4 所示。根的名字用空字符串“”来表示，但在文本中用“.”来书写。树的每一个节点都表示整个分布式数据库中的一个分区(域)，每个域可以再进一步划分成子分区(域)，每个域都有一个标签(Label)，以标明它与父域的关系。

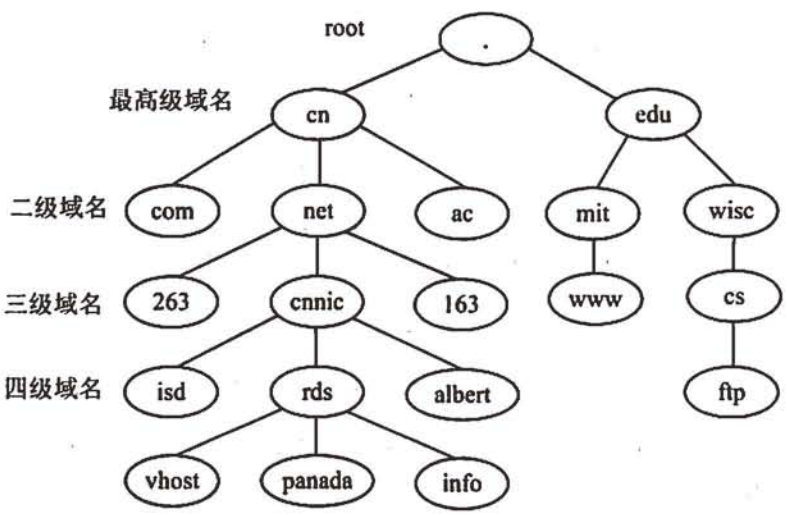


图 9.4 DNS 倒树状结构图

域(Domain)是倒树状域名空间中的一棵子树，域也有名称，称为域名(Domain Name)。域的域名同该子树根节点的域名一样，也就是说，域的名字就是该域中最高层节点的名字。举例来说，edu.cn 域的顶端就是名为 edu.cn 的节点。

在 DNS 中，域名全称是一个从该域到根的标签序列，以“.”分隔这些标签。该标签最多可包含 63 个字符。树中每一节点的完整域名为从该节点到根之间路径上的标签序列。

如果根域在节点的域名中出现，该名字看起来就像以点结尾(实际上是以点和空标签作结尾)。这些以点结尾的域名被称之为绝对域名。不以点结尾的域名被称之为相对域名。

2. DNS 域名解析过程

DNS 域名空间的域名是由分布在不同地方的域名服务器来管理的，同时 DNS 域名服务采用的是客户/服务器(client/server)工作模式。因此，DNS 解析的过程是由一个或多个的 DNS 域名服务器来完成的。

假设有一个客户机要访问 www.cnnic.net.cn 这个网站，则客户机首先要从本地 DNS 服务器获取 www.cnnic.net.cn 对应的 IP 地址，然后才能和远地服务器建立连接。

对于本地客户端的请求，本地域名服务器利用其始终运行的域名服务器进程(named)进行响应。当接收到客户请求后，就开始进行域名解析。DNS 域名解析使用的是递归查找方法，其过程如图 9.5 所示，步骤如下：

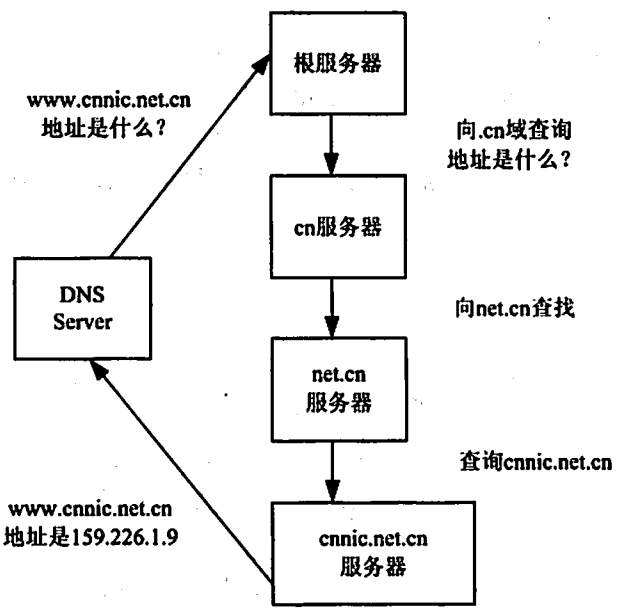


图 9.5 域名解析过程示意图

(1) 当本地 DNS 服务器接收到客户端要求解析域名 www.cnnic.net.cn 的请求之后，首先检查其缓冲区(Cache)内是否有符合的内容，如果存在(命中)则直接响应客户端的请求，否则，将请求发送给根 DNS 服务器。

(2) 根 DNS 服务器根据其顶级域名，将请求转发到.cn 域的 DNS 服务器。

(3) .cn 域的 DNS 服务器又根据其二级域名，再将请求转发到.net.cn 域的 DNS 服务器。

(4)　.net.cn 域的 DNS 服务器再根据其三级域名，将请求转发到.cnnic.net.cn 域的 DNS 服务器。

(5)　最终，.cnnic.net.cn 域的 DNS 服务器终结解析域名 www.cnnic.net.cn 的请求，并将其所对应的 IP地址返回给本地的 DNS 服务器。

(6)　本地 DNS 服务器最终将解析域名的请求结果返回给客户端。

3. FQDN

完全合格域名(Fully Qualified Domain Name，FQDN)在 DNS 域名系统中用于 Internet 上主机名称到 IP 地址的解析。FQDN 具有如下特点：

- FQDN 如同 IP 地址一样，具有惟一性。
- 一个 FQDN 对应不同的服务或者位置。
- 每一个名称都以“.”隔开。

FQDN 通常表示为：主机名＋组织机构的相关域名；这样可以惟一地标识网络上的特定服务器或设备。如 www.edu.cn，表示在 edu.cn 组织的域名上提供 Web 服务的服务器。

9.2.1.2　电子邮件

电子邮件(E-mail)无疑是 Internet 上最流行的应用程序。电子邮件来源于专有电子邮件系统。早在 Internet 流行之前，电子邮件就已经存在了。在主机多终端的主从式体系中，电子邮件是根据从一台计算机终端向另一计算机终端传送文本信息的简单方法而发展起来的。

经历了漫长的演变过程之后，电子邮件现在已经成为了一个更加复杂丰富的系统。现在，可以通过电子邮件系统传送声音、图片、图像、文档等多媒体信息，甚至于像数据库或账目报告等这些更专业的信息都可以通过电子邮件系统以附件的形式在网上转发。通常，传送信息时要指明接收方的 E-mail 地址。普通地址格式是 name@主机文本地址。

现在，电子邮件已成为许多商家和组织机构的生命血脉。毫无疑问的是，Internet 扩展了电子邮件的应用范围。过去只能在其局域网内进行交谈的公司成员，现在可以通过 Internet 网络与他们的客户、竞争伙伴以及世界上的任何人进行通信和交流。

SMTP 协议和 POP 协议是两个重要的 Internet 邮件服务协议。一旦某个企业或组织机构的电子邮件系统通过支持 SMTP 协议或 POP 协议的 Internet 网关连接到 Internet 网络上，不论该系统的电子邮件用户在何处，他们都可以和任何具有相似连接的电子邮件用户进行通信交流。

图 9.6 显示了一个电子邮件传递的过程。当用户发送邮件时，本地邮件服务器首先确定邮件的目的地址是否是本地的。如果邮件的目的地址是本地的，那么邮件服务器直接递送给指定的接收者。如果邮件的目的地址不是本地的，那么本地邮件服务器会将文件存储起来(就好象将信放在信箱里)，等待目标邮件服务器来获取。当目标邮件服务器投递邮件时，它首先与本地邮件服务器建立一个 TCP 连接。成功连接后，目标邮件服务器和本地邮件服务器进行 SMTP 分组交换，最终完成邮件的传送。目标邮件服务器获取到邮件后将其递送给指定的接收者。

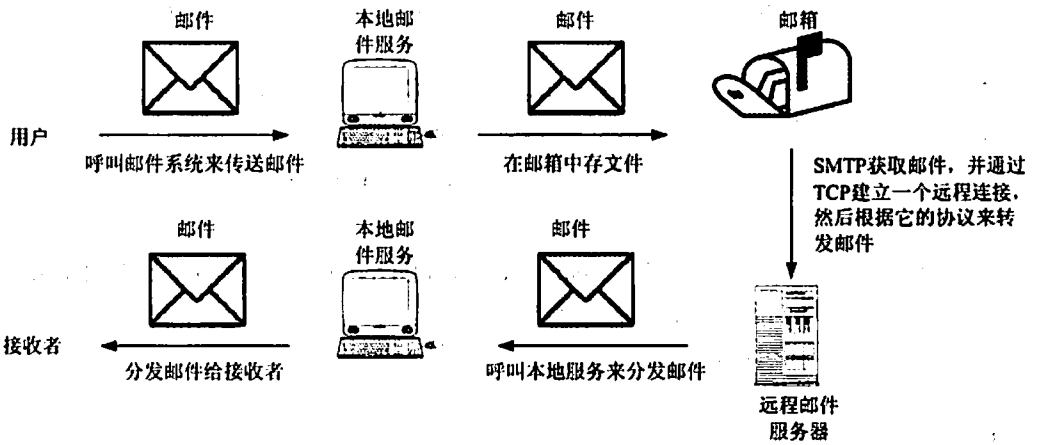


图 9.6 电子邮件传递示意图

1. SMTP 协议

简单邮件传输协议(Simple Mail Transfer Protocol，SMTP)是 TCP/IP 协议族中的标准邮件服务协议，其首要职责是确保邮件能够在不同主机间传输。

SMTP 的主要功能是标识发送方、接收方，传输消息，提供消息已经被发送的确认。SMTP 定义了一组命令用来调用其过程，例如 HELO(sic)、MAIL FROM 和 DATA 等命令。应答由一组应答代码组成，例如 250(OK)和 550(用户未知)等，应答消息通常不易懂。大多数 SMTP 实现都提供一种更加友好的用户接口，例如 Outlook 或 FoxMail 等应用软件。

在 SMTP 交互过程中，发送方在确认一个或多个接收方后才发送邮件。当 SMTP 服务器进程接收发往特定接收者的邮件后，如果用户在本地，则 SMTP 服务器要负责将邮件送到用户。如果用户不在本地，则要将邮件转发给适当的目标主机。SMTP 使用 DNS 的邮件交换(Mail Exchange，MX)记录，确定指定用户所在的适当邮件服务器。当消息通过网络传输时，需要携带反向路由信息，以使得发送方可以得到失败通知信息。

图 9.7 显示了客户和邮件服务器间的 SMTP 分组交换过程。在这里 SMTP 分组被称为 SMTP 协议的数据单元(Protocol Data Unit，PDU)。在建立了 TCP 连接后，邮件服务器发送一个 220 PDU 指出它已准备好接收邮件(编号 220 用来表示分组类型)。在客户和邮件服务器交换并确认身份后，客户发送一个 Mail From PDU 指出有邮件发送并识别发送者。如果邮件服务器接收该发送者的邮件，它将以 250 OK PDU 作为响应。在发送邮件内容前，客户还将发送一个或多个 Rcpt To PDU 指出指定的接收者，并确定接收者是否存在。

以上只是简略描述了 SMTP 协议，并没有详细讨论 PDU 格式、转发邮件等问题。如果需要 SMTP 协议详细的信息，可参考 RFC 788 和 RFC 821。

2. POP 协议

SMTP 定义了一组用于电子邮件服务器之间交换邮件消息的规则。但是，SMTP 没有提供用户访问和管理其电子邮件的明确机制。例如，SMTP 没有提供命令使用户能够回应消息、将消息转发给另一个用户或发送消息的副本。

为了填补这个空白，人们开发了邮局协议(Post Office Protocol，POP)，现在常用的是第三版，简称为 POP3。POP 协议主要用于用户本地网络。通过 POP 协议，客户机登录到

邮件服务器上后，可以删除自己的邮件或是将邮件下载到本地。POP 邮件服务器一般使用的是 TCP 的 110 号端口。

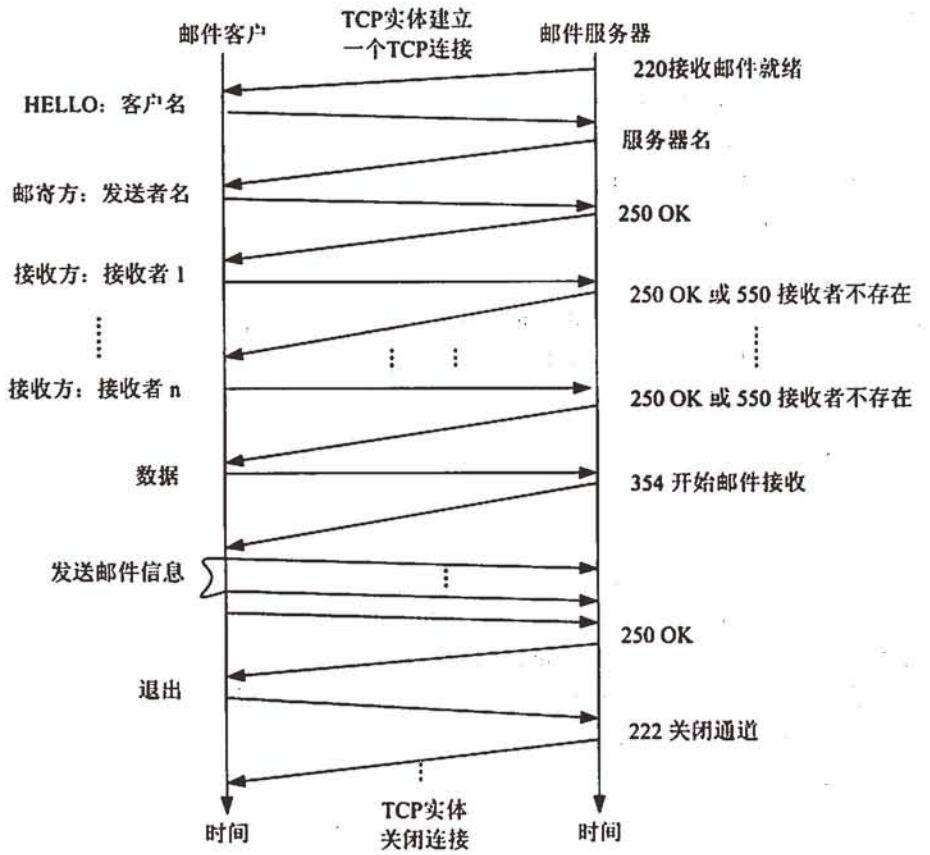


图 9.7　SMTP 分组交换流程图

3. IMAP 协议

因特网消息访问协议(Internet Message Access Protocol，IMAP)是另一个支持实现在邮件服务器上读取电子邮件的协议。通过 IMAP 协议，客户能够像访问本地消息一样地访问存储在远程邮件服务器上的邮件。现在常用的 IMAP 版本是第四版，简称为 IMAP4。

存储在 IMAP 邮件服务器上的邮件可以通过多台计算机进行远程操作，而不需要在不同计算机之间传递信息。换句话说，在家里使用笔记本电脑阅读邮件和在办公室中使用台式计算机阅读邮件时，不需要考虑各个计算机之间的同步，因为在不同计算机上阅读的邮件一直都保存在邮件服务器上。这种“在线”消息访问与“离线”的 POP 形成对比，POP 邮件访问只适合在一台计算机的情况下，邮件需要下载到本地 POP 客户端，同时还需要从邮件服务器删除邮件。

虽然 IMAP 的命令比 POP 的多，这样使得 IMAP 更难以实现和使用，但是 IMAP 相应的扩展库使其具有很好的灵活性和扩展性。很多对邮件的管理、排序和编辑功能，都可以在 IMAP 邮件服务器上实现。现在的很多 POP 客户端也都具有类似的选项，与 IMAP 相比，POP 的主要优点是使用该协议的应用系统都已经比较成熟，目前也已经有很多产品。

4. MIME

就像过去 20 多年中网络使用的数据类型发生了很大变化一样，通过电子邮件交换的信息类型也变得丰富多样。

多用途因特网邮件扩展(Multipurpose Internet Mail Extensions，MIME)就是为适应这种变化而定义的。通过 MIME 的定义使得发送方可以为电子邮件提供使用各种非文本格式作为附件成为可能。MIME 支持的媒体类型包括文本、图像、音频、视频和应用程序。

MIME 增强了在 RFC 822 中定义的电子邮件报文的能力，允许传输二进制数据。MIME 编码技术用于将数据从 8 位都使用的格式转换成只使用 7 位表示数据的 ASCII 码格式。

5. LDAP 协议

轻量级目录访问协议(Lightweight Directory Access Protocol，LDAP)通过将相关的内容存放在统一的目录之下，为用户提供基于客户/服务器工作方式的信息查询手段。

LDAP 是基于 X.500 标准的，但是比 X.500 标准简单，并且可以根据需要定制。与 X.500 不同的是 LDAP 支持 TCP/IP，这一点对于访问 Internet 是必需的。LDAP 最大的优势是：可以在任何计算机平台上，用很容易获得的而且数目不断增加的 LDAP 的客户端程序访问 LDAP 目录。

在 LDAP 中，目录是按照树形结构组织的。目录由条目(Entry)组成，条目相当于关系数据库中表的记录；条目是具有区别名 DN(Distinguished Name)的属性(Attribute)集合，DN 相当于关系数据库表中的关键字(Primary Key)；属性由类型(Type)和多个值(Values)组成，相当于关系数据库中的域(Field)。LDAP 条目由域名和数据类型组成；为了方便检索的需要，LDAP 中的 Type 可以有多个 Value。LDAP 条目的组织一般按照地理位置和组织关系进行组织，非常直观。

LDAP 把数据存放在文件中，为提高效率可以使用基于索引的文件数据库，而不是关系数据库。LDAP 协议集还规定了 DN 的命名方法、存取控制方法、搜索格式、复制方法、URL 格式、开发接口等。

6. 邮件列表

邮件列表(Mailing List)是 Internet 上的一种重要工具，用于各种群体之间的信息交流和信息发布。邮件列表具有传播范围广的特点，可以向 Internet 上的用户迅速传递消息，传递的方式可以是主持人发言、自由讨论和授权发言人发言，以及电子会议等方式。邮件列表使用简单方便，只要能够使用 E-mail，就可以使用邮件列表。

邮件列表广泛应用于企业间的通信、同学亲友之间的联系、股票信息、技术讨论、邮购业务、新闻发布、电子杂志等，涉及社会的方方面面，如：

- 电子会议　可以组织学术会议，针对具体议题进行广泛的讨论。
- 电子杂志　可以主办自己的电子杂志，通过邮件列表的方式，向数十万用户同时发送。
- 企业应用　新产品发布、与客户保持联系、产品的技术支持、信息反馈。
- Web 站点　主页更新、信息反馈。
- 组织和俱乐部　吸引新用户的加入、提供成员之间的交流工具。
- 同学和亲友　保持快速、方便的联系。

- 技术讨论 就某项技术(诸如数据库、机械模具设计、安全等)进行交流。
- 邮购业务 在网上进行远程的商务订购，多为 B2C 的模式。
- 股票信息 发布当前的股票买卖信息、趋势等。
- 产品供求信息 宣告、发布产品的需求或者所能提供的产品。

邮件列表方便快捷的特点符合当今社会人们追求个性化的需求。目前，国内比较大的专业邮件列表服务商有：希网、索易、通易等。

无论是专业性邮件列表网站，还是综合性的邮件列表网站，主要都提供以下两种服务：

- 用户申请成为邮件列表用户，进一步成为某个邮件列表的管理者，向其他用户提供邮件列表服务。
- 普通用户订阅邮件列表，成为信息的接收者。

在当今信息资源共享的时代，邮件列表无疑架起了一座“免费”的沟通桥梁。邮件列表的潜力是非常大的，不仅邮件列表广告可以带来可观的收入，而且，以后的邮件列表市场可能会实现由免费到收费的转变。相信对每个追求付出与收益的现代人来说，使用邮件列表将是一个很好的选择。

7. Web Mail

Web Mail 是指用户可以直接通过 WWW 浏览器软件来访问电子邮件服务商的电子邮件系统。

我们只需要在 WWW 浏览器上，输入该电子邮件系统的网址；然后，输入用户名和密码，进入用户的电子邮件信箱，这样就可以在 WWW 浏览器上处理用户的电子邮件。

通过 Web Mail，用户无须特别准备设备或软件，无论是哪一台电脑，只要有机会浏览因特网，即可以进入到电子邮件服务商提供的电子邮件系统处理自己的邮件。

Web Mail 的另一个好处就是不必担心因为读取含有病毒的文件而导致机器中毒，更不会有中毒后的个人邮件系统给其他联系人发送大量含有病毒的信件这种情况的发生。

9.2.1.3 电子新闻

1. 新闻组和新闻组服务器

电子新闻又称为网络新闻或新闻组(USENET 或 NewsGroups)。与 BBS 类似，它提供了一个场所，让用户可以对某个感兴趣问题展开提问、回答和评论，同时也可以进行其他信息的交流。

新闻组是一个遍及全世界的、巨大的电子公告栏系统，是一项通过网络交换信息的服务，它由个人向新闻服务器投递的新闻邮件组成。可以把 USENET 看成是一个有组织的电子邮件系统，不过在这里传送的电子邮件不再是发给某一个特定用户的电子邮件，而是发给全世界范围内的新闻组服务器的电子邮件。在这个公告栏上任何人都可以贴公告，也可以下载其中的公告，USENET 用户写的新闻被发送到新闻组后，任何访问该新闻组的人都有可能看到这个新闻。新闻组不提供其使用成员的名单，任何人都可以加入新闻组，也可以向新闻组投递新闻或阅读其中的新闻。

新闻组服务器可以被认为是新闻组的心脏，它负责接收世界各地的用户发来的文章，然后转发给其他用户。用户要进入新闻组，首先就要连接到该新闻组的服务器，新闻组服务器由公司、群组或个人负责维护，它可以管理成千上万个新闻组，每个新闻组都有一个

特殊主题。

目前，新闻组服务器是可以通过 USENET 新闻网络访问的两万多个公共新闻组的一个分配和投递源。USENET 是因特网上最大的新闻及讨论组网络。USENET 新闻组服务器利用网络新闻传输协议(NNTP)与其他的 USENET 新闻组服务器进行数据交换，并将新闻分发给拥有支持标准 NNTP 协议的新闻阅读器(如 Agent 或 Outlook Express)的用户。

USENET 是讨论性质的，它允许世界上任何地方的用户参与。由于新闻组的用户常常利用新闻组的公平、开放和 Internet 快速高效的特点，在新闻组上提出自己在生活、工作中的问题，发布自己有关学术、商业以及其他一切感兴趣的观点，这使得新闻组就像一个世界性的聊天广场，其话题覆盖了令人难以置信的各种主题，在这里用户可以找到所能想到的任何聊天话题，例如，计算机、网络、生活、娱乐、文学、体育、商业、财经、学习等诸多方面的内容。

2. 新闻组的运作模式

作为一个用户，要在数不清的服务器中的近万个新闻组中查找自己喜爱的新闻内容，订阅世界各地有关同一个主题的新闻，是在某个特定的服务器上就能完成呢？还是要看完所有服务器才能找到新闻或订阅新闻？一个新闻组服务器是不可能把所有新闻组的内容全都装进自己的系统的，因为这些不断增加的新闻内容会用尽为它们准备的所有存储空间。但是为了能让世界各地的用户看到某一台服务器上的新闻内容，服务器的管理程序一边同用户打交道以保证用户的信息需求，另一边同与它直接沟通的新闻组服务器不停地进行信息交流：将自己没有的新闻复制过来，将别人没有的内容复制过去。当然，这种新闻复制不是没有选择的，例如：某服务器只要有关计算机方面的 10 天以来的新闻内容，其他内容不要。这就是说：一台新闻组服务器可能只有某些新闻组而不是全部，但它所拥有的新闻组中的新闻却是来自世界各地的。

新闻组的运作模式可以用来简要说明为：服务器甲和服务器乙是两个位于不同地方的新闻组服务器，它们各自设有自己的新闻组服务项目，客户 A 和客户 B 是两个位于不同地方的新闻组用户。客户 A 使用服务器甲下载新闻，它也通过服务器甲发布新闻的；客户 B 以同样的方式使用服务器乙。如果服务器乙需要客户 A 上传到服务器甲的新闻，那么新闻将由服务器甲传送给服务器乙。因此，客户 B 只要在服务器乙上就有可能看到 A 发送的新闻内容。

由此可见，您要订阅某一特定的新闻组，只需要找一个有这个新闻组的服务器，绝对没有必要为了看世界各地的新闻而跑遍世界各地的新闻服务组器。

3. NNTP 协议

网络新闻传输协议(Network News Transfer Protocol，NNTP)是电子新闻的主要传输协议，其工作过程类似于 SMTP。NNTP 用于在协作主机之间发布新闻文章。NNTP 是一个使用可靠性连接(TCP)的应用协议，默认使用 TCP 的 119 号端口，RFC 977 文档对它进行了详细地描述。

NNTP 也像其他的 Internet 应用(HTTP、FTP、SMTP 等)一样，属于客户/服务器(C/S)模式。客户发送请求命令给服务器，服务器返回数值的响应码，并紧跟着可选的数据(取决于客户的命令)。

NNTP 使用的指令和应答都是由 ASCII 码字符集组成。传输服务使用 8 位字节传送，当在 8 位字节中有 7 位作为数据正常传送时，最高位清零。

指令由一串命令(ASCII 码)字符组成，在有些时候指令还需要附加参数。指令附加参数时，参数和指令必须由一个或几个空格分隔开。命令行必须包括所有必要的参数，并只能包含一条命令。指令和参数都不区分大小写，简单的说，就是一个指令和参数字符可以用大写，也可以用小写，或者大小写混合。

每个命令行必须以一对回车换行符(CR-LF)结束。每个命令行长度都不能超过 512 个字符，这包括空格、分隔符、标点符号和回车换行符等，因此命令和参数字符的长度实际上最多只能有 510 个字符。NNTP 不接受超出长度规定的命令行。

9.2.1.4　Web 应用服务与 HTTP

1. Web 应用服务

Web 服务器接受来自 Netscape 和 Internet Explorer 等浏览器的客户请求，通过 URL 定位到相应的宿主文件服务器上，找到相应的文件后从宿主文件服务器上下载该文件，然后通过 HTTP 协议把它传输给 Web 浏览器。这是 Web 应用服务的一个基本工作过程。

目前主要的 Web 服务器产品包括 Apache、Microsoft IIS、iPlanet Web Server 等。

Web 应用服务非常重要的一个扩展是引入了动态内容，比如，Web 服务器可以根据用户输入的请求，去直接或间接地创建新的 Web 网页，然后返回给 Web 浏览器。

最初，动态内容是通过应用 CGI(公共网关接口)方法来实现的。CGI 对 Web 服务器上程序的运行以及 Web 服务器同 Web 浏览器之间动态内容的传输进行了基本的定义。如今已经有许多服务器端的技术来扩展和提高服务器发送标准 HTML 网页的能力，比如 PHP、JSP、ASP 等。

在 Web 服务的构成中有四个重要部分，它们是 URL、HTML、XML 和 HTTP。

统一资源定位符(Uniform Resource Locators，URL)是万维网上使用的标准寻址机制，确定信息在网络上的位置。下面举一个说明标准 URL 格式的例子：http://www.edu.cn。这里“http://”表示要使用超文本传输协议，并且从叫做 edu 的网站的 www 服务器上传输信息，这个网站属于中国(.cn)。统一资源定位符 URL 不仅能够指向文本，而且还能够指向电影片断、图像文件、音乐等。如果信息能够被数字化并存储在硬盘或 CD-ROM 上，也可以使用 HTML 格式并通过 URL 访问，同时可以使用 HTTP 下载到进行查询的系统。

超文本标记语言(Hyper Text Markup Language，HTML)是编写统一标准格式文档的程序设计语言。这种标记语言由格式命令组成，使用户能够在页面上指定标题、文本段落的位置、字号、颜色、对齐方式和间隔、动画序列、引文以及能够访问其他超文本文档的按钮等。

可扩充标记语言(eXtensible Markup Language，XML)被认为是下一代 HTML。与 HTML 一样，XML 也使用格式命令；同时，XML 允许用户定义这些命令的含义。XML 能够更密切地集成数据库和用户应用系统，并且最终扩展万维网的能力。

超文本传输协议(Hyper Text Transfer Protocol，HTTP)被广泛应用于 Web 应用，它是 Web 服务的网络传输技术之一，接下来的部分将重点介绍 HTTP 协议。

2. HTTP 协议

HTTP 最初只是一个面向对象的应用级协议，而并非专用于超文本、超媒体的传输，但其精巧快速，特别是通用、无状态性以及面向对象的特点，使之非常适合于分布式协作化超文本、媒体系统。因此取名为超文本传输协议。其实 HTTP 经过扩展可用于许多任务当中，如名字服务器、分布式对象管理系统等。当前 HTTP 广泛用于 Internet，在 Web 服务器和客户机之间提供超文本链接。

超文本技术随着 20 世纪 80 年代多媒体计算机技术的兴起而蓬勃发展起来。超文本提供了将“声、文、图”结合在一起、综合表达信息的强有力手段。同时，作为一种接口技术，超文本提供了非常直观、灵活的人机交互方法，开拓了许多应用领域。理解超文本最简单的方法就是与传统文本相比较。传统文本，无论是书本，还是计算机的文本文件，都是线性的，读者在阅读时，必须一页一页按顺序地读，读者没有选择的余地。超文本与此不同，它不是一个线性的结构，而是一个非线性的网状结构。在制作超文本时，可将写作素材按其内部的联系划分成不同层次、不同关系的模块单元，然后用制作工具将这些模块单元组成一个网状结构。读者在阅读时，就不必像读线性文章时以顺序方式向下读，而是有选择地读自己感兴趣的部分。

(1) HTTP 的运作方式及消息结构

HTTP 支持客户机(浏览器)与服务器间的通信，相互传送数据。一个服务器可以为分布在世界各地的许多客户机服务。HTTP 采用请求、响应的握手方式，其基本的运作由以下四步组成：

① 连接：客户机与服务器建立连接。

② 请求：客户机向服务器提出请求。

③ 响应：如果请求被接收，那么服务器将返回应答，在应答中包括状态码和所要的响应信息。

④ 关闭：客户机与服务器断开连接。

其中“客户机”与“服务器”是一个相对概念，只存在于某个特定的连接期间，而非专用程序，即在某个连接中的“客户机”在另一个连接中可能作为“服务器”。这也就是说对于 HTTP 中的程序，应具有“客户机”与“服务器”的双重功能。在 Internet 上的通信一般是建立在 TCP/IP 连接上的，HTTP 的连接也不例外，其默认端口是 TCP 80，当然其他端口也可以使用。

HTTP 的消息有两类，即“客户机”发出的请求消息与“服务器”发出的响应消息。HTTP 的请求消息采用了开放式的方法库形式，即方法可以扩充。用方法表示请求的目的，用 URI(Uniform Resource Identifier)表示某个方法用在哪个资源上，消息的传送格式与 Internet Mail(Internet 邮件)和 MIME(Multipurpose Internet Mail Extensions，多用途 Internet 邮件扩展)相似。

完整的请求消息格式如下：

```
请求消息 = 请求行 *(通用信息头 | 请求头 | 实体头) CRLF (实体内容)
请求行 = 方法请求 + URI + HTTP + 版本号 + CRLF
方法 = “GET” | “HEAD” | “POST” | 扩展方法
URI = 协议名称 + 宿主名 + 目录与文件名
```

完整的响应信息格式如下：

响应信息 = 状态行 *(通用信息头 | 响应头 | 实体头) CRLF (实体内容)
状态行 = HTTP 版本号 + 状态码 + 原因叙述

(2) HTTP 的主要特点

① 简单

HTTP 本身既简单，又能有效地处理大量请求。在客户机与服务器连接后，客户机必须传送的信息只是请求方法和路径。正是因为 HTTP 协议简单，使得 HTTP 服务器程序规模小，而且简单。因此经由 HTTP 的通信速度很快，与其他协议相比，时间开销小得多。

② 灵活

HTTP 允许传输任意类型的数据对象。ContentType 表示正在传输数据的数据类型。如果把数据看成是在“罐”里的东西，那么 ContentType 是贴在罐上的标签，它告诉用户里面装的是什么东西。

③ 无连接

HTTP 是一个无连接协议。它的含义是限制每次连接只处理一个请求，客户机与服务器连接后提交一个请求，在客户机收到应答后马上断开连接。使用这种无连接协议，在没有请求时，服务器不会在那里闲等着，服务器更不会在完成一个请求后还把着原来的请求不放。对于无连接协议而言，服务器一方实现起来比较容易，另一方面又能充分利用网上的资源。

④ 无状态

HTTP 是无状态的协议。这既是优点也是缺点。一方面，由于没有状态，协议对事务处理没有记忆能力。如果后续事务处理需要前面处理的有关信息，那么这些信息必须在协议外面保存，势必导致每次连接要传送较多的信息。另一方面，也正是由于缺少状态使得 HTTP 累赘少，运行速度高，服务器应答快。

⑤ 元信息

HTTP1.0 对所有事务处理都加了头信息。也就是说，在主要数据前加上一块信息，我们称之为元信息，即信息的信息。它使服务器能够提供传送数据的有关信息。例如，传送对象是哪种类型，是用哪种程序语言构造的等。人们还可以利用这些元信息进行有条件地请求，或者报告一次事务处理是否成功等。

9.2.2 典型例题分析

例　阅读以下说明，回答如下问题。(2004 年下半年下午试题三)

【说明】

在 IMail 管理器中，选中 MailUser 邮件主机，然后在它右边的面板中选中 General 选项卡，出现邮件主机的配置窗口如图 9.8 所示。

如果在 IMail 管理器中，选中 User1 用户，然后在它右边的面板中选中 General 选项卡，则邮件主机的用户配置窗口如图 9.9 所示。

【问题】

1. 限制 MailUser 邮件主机里每个用户的邮箱大小不超过 10MB，如何配置？

2. 限制 MailUser 邮件主机里最多允许有 2000 个邮件用户，如何配置？

3. 限制 MailUser 邮件主机里所有用户接收的单个邮件的大小不超过 5 MB，如何配置？

4. 限制 MailUser 邮件主机里每个用户邮箱里所能存放的最多邮件数量不超过 20 个，如何配置？

5. 如何暂时禁用某个用户账号？

6. IMail 安装完成后，系统自动建立了一个名为 root 的用户，在默认情况下 root 用户是个失效的账号，如何设置使其生效？

7. 如何设定邮件自动转发？如果向多个邮件地址进行邮件自动转发，如何配置？

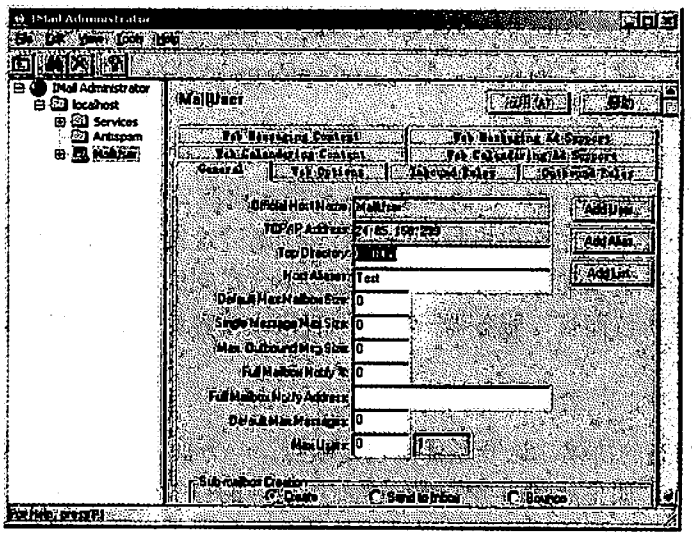


图 9.8 IMail 软件用户配置窗口(1)

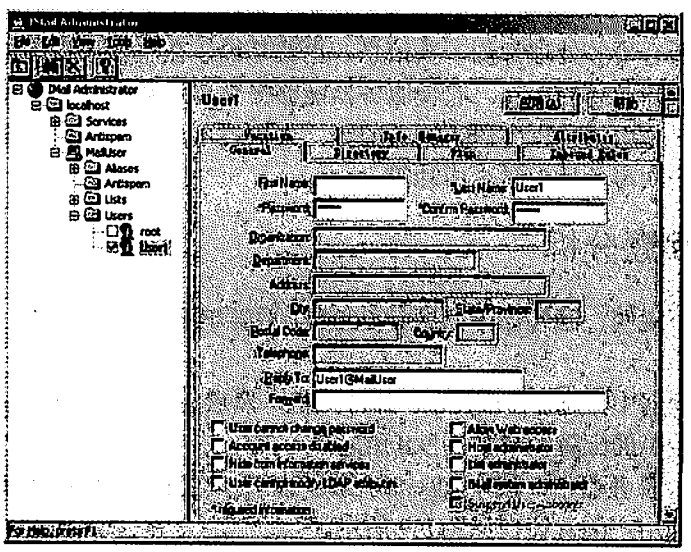


图 9.9 IMail 软件用户配置窗口(2)

分析：这是一套典型的软件操作考核题，要求考生掌握 IMail 软件的配置与管理，因此考生平时要关注常用网络应用软件的使用。比如：Notes、qmail、postfix 等邮件系统。

IMail 是当今最流行的电子邮件服务器端软件之一，受到了众多专业和非专业人士的青睐。IMail 是一个高性能的、基于标准的 SMTP/POP3/IMAP4/LDAP 的邮件服务器。具有简单直观的图形用户界面，非常易于管理。主要特色包括：多域名支持、远程管理、Web 邮件、可创建邮递清单(mailing lists)、反垃圾邮件支持、病毒防护等。操作很简单，但功能异常强大。用它可以很方便地在自己的主机上创建一个邮件服务器。

在 IMail 管理器中，选定 localhost，然后右击并在弹出的快捷菜单中选择 Add Host 命令，即可进入邮件主机的配置窗口。然后选中你的机器的 IP 地址，将其对应的 Official Host Name 改成你需要的域名，再单击 Save 按钮保存，遇有提示一律选 Yes，最后用 Exit 命令退出此配置窗口即可。

在 IMail 管理器中，选中此邮件主机，然后在它右边的面板中选 general 选项，再将 Default Max Mailbox Size 的值(单位为字节)改成需要的大小即可。限制某个邮件主机里每个用户的邮箱大小，如此值为 0 则表示不限制。通过修改 Single Message Max Size 的值，就可以限制某个邮件主机里所有用户接收的单个邮件的大小。修改 Default Max Messages 的值即可限制某个邮件主机里每个用户邮箱里所能存放的最多邮件数量。修改 Max Users 的值即可限制某个邮件主机里最多能有几个邮件用户。

在 IMail 管理器中，选中欲删除的主机名并右击，在弹出的快捷菜单中选择 Delete 即可删除一个邮件主机。如要增加一个有 IP 地址的邮件主机，首先需要将此邮件主机域名设置好相应的 DNS，再将相应的 IP 地址指向它即可。

现在让我们来看看 IMail 邮件系统的账号管理。在 IMail 管理器里，选中此邮件主机下的 Users 项，然后在右边面板中即可修改某个邮件主机里所有用户的默认权限设置。这些修改后的值将成为以后增加的所有用户的初始权限值。

默认的情况下，用户 root 是失效的。要使它生效，则需要在 IMail 管理器里选中它，然后选中右边面板中的 General，把其下的 Account Access Disabled(账号禁用)前的小勾去掉，再单击 Apply 即可。如果要禁用某个邮件账号，我们只需要选定相应用户名，然后在这个用户所对应的右侧属性中的 Account Access Disabled 打上勾即可。

当需要禁止某个邮件账号进行 Web 方式来登录时，则去掉用户名所对应的 Allow Web access(接受 Web 方式)前的小勾即可。而如果需要让某个账号来管理这个邮件系统的时候，则可选择该用户，然后赋予它(即选中)Allow Web access 和 IMail system administrator(系统管理员)的权限。

当需要修改某个用户的密码时，选 Password 输入新密码，再在 confirm 中重输一次密码即可。在用户右侧的属性里面，可以使用 Reply To 的功能来改变回复的邮件地址，而 Forward 功能则用于转发到的目标地址；多个转发地址间用英文逗号分隔。默认的，邮件自动转发后原邮箱里不会保存。

对于用户邮件的相关限制，IMail 可以做到如下功能。选中用户后，右边面板中选 Max Mailbox Size(最大邮箱尺寸)，将它修改成需要值即可限制某个用户的邮箱大小，单位为字节；如果大小为 0 则表示不限制。修改 Max Mailbox Msgs(最多邮件数)中的值即可限制某个用户在邮件主机上同时存放的最多邮件数目；大小为 0 表示不限制。通过 Total Size 可查

看一个用户的邮箱使用情况，Total Size 为已有所有邮件的总大小(字节)；Total Msgs 为已有邮件的总数；Files 为已有文件的总数。

以上仅仅是 IMail 的简单介绍，详细功能还需要细细体味，多多练习。

答案：

1. 将图 9.8 中的 default max mailbox size 设置为 10MB。
2. 将图 9.8 中的 max users 设置为 2000。
3. 将图 9.8 中的 Single Message max size 设置为 5MB。
4. 将图 9.8 中的 default max messages 设置为 20。
5. 在图 9.9 中选中 Account access disabled(即在该项前面的方框里打勾)。
6. 与在图 9.9 中设置 user1 一样，对 root 用户账号进行设置，这样就可以使其变得可用。
7. 在图 9.9 的 Forward 中设定转发地址。

9.2.3 同步练习

1. TCP/IP 协议的传输层有__(1)__和__(2)__协议。其中是__(3)__面向连接的协议，是__(4)__面向无连接的协议。
2. 目前，最常使用的网络管理协议是_____。
3. 在因特网电子邮件系统中，电子邮件应用程序发送邮件通常使用__(1)__协议，而接收邮件通常使用__(2)__协议。电子邮件服务采用__(3)__工作模式；电子邮件由__(4)__、__(5)__两部分组成。
4. 电子新闻常通过__(1)__协议来传输。这协议是面向__(2)__的应用协议，其使用知名服务的端口号是__(3)__。

9.2.4 同步练习参考答案

1. (1)TCP (2)UDP (3)TCP (4)UDP
2. 简单网络管理协议(SNMP)
3. (1)SMTP (2)POP3 (3)客户机/服务器
   (4)邮件头 (5)邮件体
4. (1)网络新闻传输协议(NNTP) (2)有连接 (3)119

9.3 负 载 分 布

9.3.1 考点辅导

负载分布，又称为负载均衡，它是由多台服务器以对称的方式组成一个服务器集合，每台服务器都具有等价的地位；通过某种负载均衡技术，将外部发送来的请求均匀地分配到对称结构中的某一台服务器上，而接收到该请求的服务器将独立地回应客户。

负载均衡利用现有的网络结构，提供一种高效、透明的方法扩展网络设备和服务器的

带宽，增加吞吐量，加强网络数据处理能力，提高相关业务的可扩展性、灵活性以及稳定性。

9.3.1.1　常用负载均衡技术

常用的负载均衡技术有：基于 DNS 的负载均衡、基于反向代理的负载均衡和基于 NAT 的负载均衡。

1. 基于 DNS 的负载均衡

通过 DNS 服务中的随机名字解析来实现负载均衡。在 DNS 服务器中，可以为多个不同的 IP 地址配置同一个名字，而最终查询这个名字的客户机将在解析这个名字时从 DNS 服务器中得到其中一个 IP 地址。因此，对于同一个名字，不同的客户机会得到不同的 IP 地址，从而访问不同地址上的 Web 服务器，以达到负载均衡的目的。

2. 基于反向代理的负载均衡

通过代理服务器可以将请求均匀地转发给多台内部 Web 服务器中的一台，从而达到负载均衡的目的。这种代理方式与普通的代理方式有所不同，标准代理方式是客户使用代理访问多个外部 Web 服务器，而这种代理方式是多个客户使用它访问多个内部 Web 服务器，因此也被称为反向代理模式。

3. 基于 NAT 的负载均衡

网络地址转换(NAT)指的是在内部地址和外部地址之间进行转换，以便具备内部地址的计算机能访问外部网络，而当外部网络中的计算机需要访问地址转换网关所拥有的某一外部地址时，地址转换网关能将其请求转发到一个映射的内部地址上。因此如果地址转换网关能将每个连接均匀转换为不同的内部服务器地址，此后外部网络中的计算机将与各自对应的服务器进行通信，从而达到负载分担的目的。

9.3.1.2　Web 交换

为应付不断增加的负载和新的应用需求，Web 交换机应运而生。Web 交换机可为数据中心设备(包括互联网服务器、防火墙、高速缓冲服务器和网关等)提供负载均衡。由于可在应用层为电子商务提高性能、增强安全性、可用性和扩充能力，Web 交换机已成为新型互联网数据中心基础设施中不可或缺的设备。

起初，Web 交换机采用 L4(四层)交换技术。四层交换技术利用 OSI 开放模型的第三层(网络层)和第四层(传输层)包头中的信息——包括 TCP/UDP 协议以及其端口号、标记应用会话开始与结束的“SYN/FIN”位以及源/目的 IP 地址，进行应用数据流会话的识别，能够让四层交换机做出向何处转发会话传输流的智能决定。

除了提供传统第二或第三层交换机所提供的连接和数据包路由服务外，Web 交换机还可提供传统局域网交换机和路由器所缺乏的完备的策略(将局部和全球服务器负载均衡、存取控制、服务质量保证(QoS)及带宽管理等结合起来)。目前，Web 交换技术已由纯粹的传输层(第四层)设备发展到具有基于内容的(第七层)智能交换。

基于内容的智能交换逐渐成为新互联网数据中心基础设施的指定传输管理服务，它们能让电子商业机构为新的商业需求架构其服务器及应用程序体系结构，并快速作出反应。下面将介绍 Web 内容智能交换的基本原理(如图 9.10 所示)。

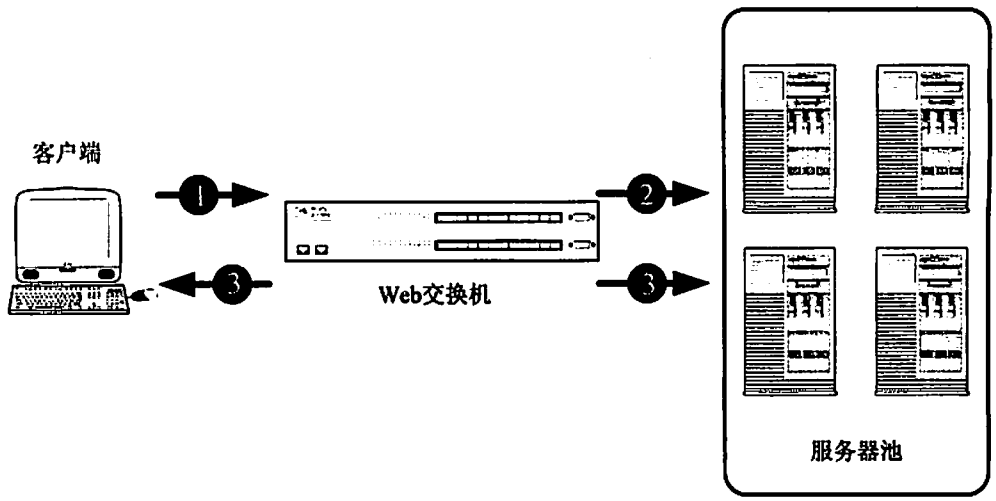


图 9.10 内容智能交换原理图

首先，内容请求的解析需要临时终止来自客户端的 TCP 连接。换句话说，Web 交换机必须先“假装”自己为服务器，并询问客户端需要什么，然后检验请求：

(1) 客户机向一个虚拟 IP 地址(VIP，Web 交换机上的一个 IP 地址)发送请求，进行 TCP 的“握手”。

(2) Web 交换机代表后台的服务器完成 TCP 的连接设置，并记录好顺序号。

(3) 客户机向 VIP 发送第一组 HTTP GET。

其次，Web 交换机建立到适当服务器的连接；在这个过程中，Web 交换机必须临时将请求保存在缓冲区：

(4) Web 交换机捕获并解析 URL，通过某种负载均衡算法选择最佳的后台服务器。

(5) Web 交换机向选择好的后台服务器发起 TCP 的“握手”。

(6) Web 交换机记录好此顺序号。

(7) Web 交换机转发刚刚缓存的客户机的 GET 的请求。

最后，Web 交换机建立客户机请求与服务器响应的对应关系；然后，进行数据的快速转发。

(8) Web 交换机对每个数据包重新封装，执行顺序号的调整，并且进行 TCP/IP 的检查和计算以及完成 NAT。

使用内容智能交换技术具有如下优点：

① 灵活地放置内容

Web 交换机通过检验 Web 请求的 URL，可确定请求的内容和类型，并将该请求复位定向到存放该请求 URL 的服务器上。利用内容智能交换，网站内容可在不改变应用程序的前提下被分离。这样，每台服务器只需要拥有部分而不是全部内容，这样也有利于部署专用、特定内容类别或处理功能的服务器。

② 提高网站的性能

不具备 Web 内容智能交换的第四层 Web 交换机，只会将每个 TCP 连接的所有 HTTP 1.1 请求转发给同一台服务器。相反，内容智能交换机则可将 TCP 连接上的各个请求，转发到

不同服务器，提高负载分布的分散性。这样可以优化资源的利用率，提高网站的整体性能。

③　提高服务器的利用率(命中率)

因为在本机内存中取出资料要比在后端数据库或硬盘中取资料快很多，所以在会话过程中，服务器会将最近使用过的资料存储于内存中。Web 交换机可以将具有相同网络跟踪器的请求发送给同一台服务器，利用服务器高速缓冲存储器来提高服务器的效率和性能。

④　加强优先级别的服务及带宽管理

利用智能交换技术，Web 交换机可以根据传输不同的内容类别——视频、声音、文本等，分配网络带宽、克服网络延时。同样，也可以根据用户的类别(例如，经常购物的用户或是经常浏览却很少购物的用户)为用户提供不同优先级别的服务。此时，Web 交换机必须能够识别用户浏览器软件中的 Cookie 信息。

9.3.2　典型例题分析

例　阅读以下说明，回答问题。(2003 年下午试题三)

【说明】

网络地址转换(NAT)的主要目的是解决 IP 地址短缺问题以及实现 TCP 负载均衡等。在图 9.11 的设计方案中，与 Internet 连接的路由器采用了网络地址转换。

【问题】

请根据路由器的 NAT 表(表 9.1)和图 9.11 中给出的网络结构、IP 地址，简要叙述主机 B 向内部网络发出请求进行通信时，边界路由器实现 TCP 负载均衡的过程。

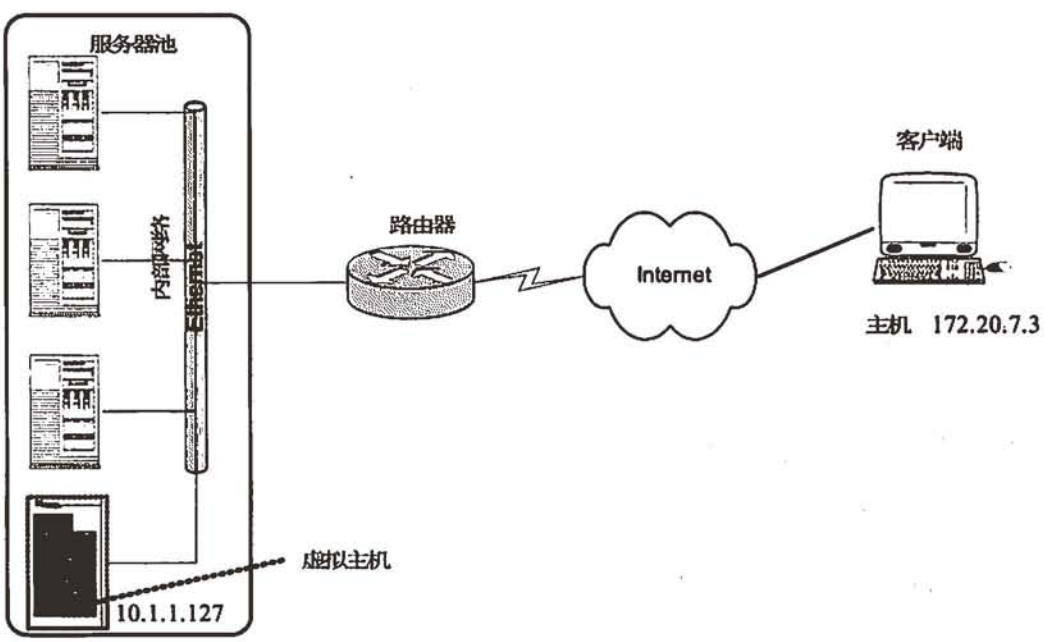


图 9.11　互联网络拓扑图

表 9.1 路由器的 NAT 表

协 议	内部局部地址及端口号	内部全局 IP 地址及端口号	外部全局 IP 地址及端口号
TCP	10.1.1.1:80	10.1.1.127:80	172.20.7.3:3058
TCP	10.1.1.2:80	10.1.1.127:80	172.20.7.3:4371
TCP	10.1.1.3:80	10.1.1.127:80	172.20.7.3:3062

分析：通过使用 NAT 进行数据流的负载均衡，其主要是在内部地址和外部地址之间进行转换然后分配请求。当外部网络中的计算机需要访问地址转换网关所拥有的某一外部地址时，地址转换网关能将其请求转发到一个映射的多个内部地址的其中一个。因此如果地址转换网关能将每个连接均匀转换为不同的内部服务器地址，此后外部网络中的计算机就可以各自与自己转换得到的地址上的服务器进行通信，从而达到负载分担的目的。

如图 9.11 所示，对外提供 Web(80 端口)服务的是以虚拟主机——IP 地址为 10.1.1.127 的身份来实现的。而虚拟主机实际调用了由后台三台现实主机(10.1.1.1，10.1.1.2，10.1.1.3)构成的服务器池。当外部向 IP 10.1.1.127 做 80 端口的请求时，路由器将从后台的 POOL 里选取实际主机来提供服务。

答案：路由器实现 TCP 负载均衡的过程如下：

(1) 外部主机 B(172.20.7.3)发出请求，建立 B 到虚拟主机(10.1.1.127)的连接。

(2) 边界路由器接到这个连接请求后，查询 NAT 表，建立一个新的地址转换映射。如：为 10.1.1.127 分配真实主机地址 10.1.1.1。

(3) 边界路由器用所选真实地址替换目的地址，转发该数据包。内部主机 10.1.1.1 接收到该数据包，并作应答。

(4) 边界路由器接到应答包后，根据内部地址及端口号和外部地址及端口号，从 NAT 映射表中查找对应的内部虚拟主机地址及端口号。

(5) 将源地址转换为虚拟主机地址，并转发应答包；B 接收到源地址为 10.1.1.127 的应答包。

(6) 下一个请求时，边界路由器为其分配下一个内部局部地址，如 10.1.1.2。

9.3.3 同步练习

1. 常用的负载均衡技术有哪几种。
2. 简述 Web 交换的基本技术。

9.3.4 同步练习参考答案

1. DNS 轮询技术、反向代理技术、基于 NAT 技术。

2. Web 交换利用网络层的源/目的 IP 地址以及传输层的包头中的信息——包括 TCP/UDP 协议及其端口号、标记应用会话开始与结束的“SYN/FIN”位。当前，Web 交换已经发展到使用内容智能交换——第七层的交换技术。

9.4　电子身份验证

9.4.1　考点辅导

随着互联网和信息技术的不断发展，信息的安全性问题开始引起了人们的密切关注。电子身份验证作为 Internet 安全的一个重要方面，影响着 Web 站点、电子商务、电子政务等众多互联网的应用。

9.4.1.1　身份认证

电子身份验证指的是用户向系统表明自己的身份证明过程。身份认证指的是系统查核用户的身份证明的过程(实质上是查明用户是否具有他所请求资源的使用权限)。通常将这两种过程统称为身份认证。

当前，许多应用系统都使用传统的单元素认证模式，即："用户名＋口令"。这种认证模式的安全性非常弱，用户名和口令易被窃取而导致损失；而且"用户名＋口令"的认证模式，用户使用起来也非常不方便，用户常常需要记住复杂的用户名和口令。因此传统的单元素认证模式已远远不能满足许多系统的安全性要求。电子身份认证系统可以替换原有的"用户名＋口令"的简单认证模式，也可与原有的认证模式结合，形成双元素认证，即"实物＋信息"，来满足应用系统更高层次的安全性要求。这里的"实物"包括：智能令牌、IC 卡、磁卡、生物信息等。

身份认证是实现网络安全的重要机制之一。在安全的网络通信中；涉及到的通信各方必须通过某种形式的身份验证机制来证明各自的身份，验证用户的身份与所宣称的是否一致，然后才能实现对于不同用户的访问控制和记录。

电子身份认证被广泛应用于电子商务和电子政务中。例如：支付型和非支付型的电子商务活动，包括传统的商业、制造业、流通业的网上交易，以及公共事业、银行保险证券、社保医疗民政、人事劳动用工、工商税务海关、政府行政办公、教育科研单位等部门的网上申报、网上审批、网上办公等。

9.4.1.2　电子证书

电子证书(Key)，又称数字证书或 CA 证书，它是电子身份认证实现的一个重要工具。它是目前国际上最成熟并得到广泛应用的信息安全技术。通俗地讲，电子证书就是个人或单位在网络上的身份证，它包含有网络用户身份信息的一系列数据，用来在网络通信中识别通信各方的身份。

电子证书由权威性的、公正的、第三方认证机构来颁发和管理，这个权威性的证书管理机构就是认证中心(Certificate Authority)，简称 CA。

电子证书的格式遵循 ITUT X.509 国际标准；X.509 电子证书通常包含以下内容：

- 证书的版本信息。
- 证书的序列号，每个证书都有惟一的证书序列号。
- 证书所使用的签名算法。

- 证书的发行机构名称，命名规则一般采用 X.500 格式。
- 证书的有效期，通用的证书一般采用 UTC 时间格式，其计时范围为 1950-2049。
- 证书所有人的名称，命名规则一般采用 X.500 格式。
- 证书所有人的公开密钥。
- 证书发行者对证书的签名。

电子证书解决了网络信息传输中的机密性问题，防止传送的信息被篡改，同时也可以确定对方的真实身份和信息的真实性，达到互相了解的目的，从而更好地保护双方的商业秘密和利益，确保网络经济的诚信资质。

9.4.1.3 数字签名与公钥系统

电子身份验证系统通过诸如数字签名、数字信封、时间戳服务等技术手段，在 Internet 上建立起有效的信任机制。下面将详细说明数字签名的具体实现。

数字签名是指用户使用自己的私钥对原始数据的哈希(Hash)摘要进行加密所得到的数据。数字签名实现的基础就是加密技术。

在网络应用中一般采取两种加密形式：对称密钥加密和公开密钥加密。其中，公开密钥加密得到更广泛的应用。在公开密钥加密系统中，加密密钥和解密密钥是不同的。一般对于每个用户生成一对密钥后，将其中一个作为公钥公开，另外一个则作为私钥由属主保存。公钥加密算法的加密强度很高，同时数字签名还与每次被传送的数据和时间等因素有关，而且并不要求通信双方事先要建立某种信任关系或共享某种秘密，因此公钥加密算法十分适合在 Internet 网上使用。

常用的公钥加密算法是 RSA 算法，其数学原理是将一个大数分解成两个质数的乘积，加密和解密用的是两个不同的密钥。即使已知明文、密文和加密密钥(公开密钥)，想要推导出解密密钥(私密密钥)，在计算上也是不可能的。我们将以发送一份保密文件为例，说明公钥加密算法的实现步骤：

(1) 发送方将报文按双方约定的 Hash 算法，计算得到一个固定位数的报文摘要。在数学上保证，只要改动报文中任何一位，重新计算出的报文摘要值将会与原先的值不相符，这样就保证了报文的不可更改性。发送方将该报文的摘要值，用自己的私密密钥加密，然后连同原报文一起发送给接收方，产生的报文即被称为数字签名。

(2) 接收方收到数字签名后，使用同样的 Hash 算法对报文计算摘要值。同时也使用发送方的公开密钥，对加密的文字变换进行解密。如果解密后的文字变换和接收方自己产生的文字变换一致，那么接收方就可以相信发送方的身份，因为只有发送方的私密密钥能够产生加密后的文字变换。

(3) 当发送方需要验证接收方的身份时，接收方根据自己的私密密钥创建一个新的数字签名，然后重复上述过程。

一旦发送方和接收方互相确定了对方的身份，那么他们就可以进行安全地通信。

公开密钥体系的一个突出优点是：它解决了密钥发布的管理问题，客户可以公开其公开密钥，而保留其私密密钥。公开密钥的公布可以通过第三方证明授权认证中心(CA)来完成。

9.4.2　典型例题分析

例　阅读以下说明，回答问题。

【说明】

电子身份验证有多种机制：基于 DCE/Kerberos 的认证机制、基于公共密钥的认证机制、基于挑战/应答的认证机制等。而使用比较多的是基于公共密钥认证机制的身份验证。

【问题】

图 9.12 描述了基于公共密钥的认证机制的身份验证的数字签名的最后验证过程——身份验证是否通过。

1. 描述数字签名的获得的过程，是接收方创建还是发送方创建？
2. 接收方是如何进行验证操作的？

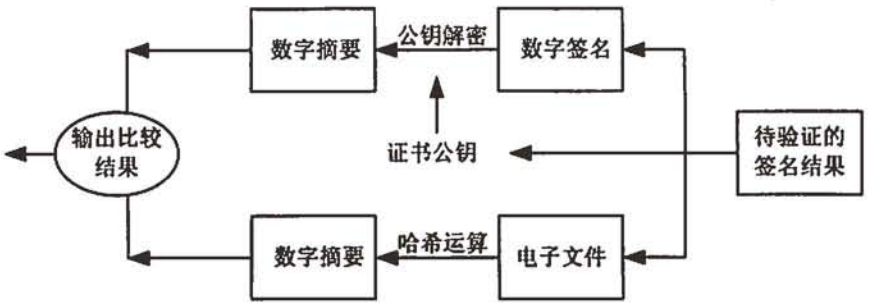


图 9.12　数字签名流程图

分析：基于公共密钥的认证机制的身份验证的基本原理是将原文用非对称密钥加密传输。其详细过程如下：

(1) 发送方将原文信息进行哈希 HASH 运算——单向不可逆的变换，得一哈希值即数字摘要 MD。

(2) 发送方用自己的私钥 PVA，采用非对称 RSA 算法，对数字摘要 MD 进行加密，即得数字签名 DS。

(3) 发送方将原始的文字信息和加密后的数字签名 DS 传送给指定的接收方。

(4) 接收方接受到数字签名的结果，其中包括数字签名、电子原文等。

(5) 接收方用同样的 Hash 算法对电子原文计算，得到数字摘要 MD1。

(6) 接收方用发送方公钥 PBA 解密数字签名 DS，导出数字摘要 MD2。

(7) 接收方将两个数字摘要 MD1 和 MD2 进行比较，验证原文是否被修改。如果二者相等，说明数据没有被篡改，是保密传输的，签名是真实的；否则拒绝该签名。

答案：

1. 数字签名操作具体过程是：首先生成被签名的电子文件，然后对电子文件用哈希算法做数字摘要，再对数字摘要用签名私钥做非对称加密，即作数字签名；最后是将以上的签名和电子文件原文以及签名证书的公钥加在一起进行封装，形成签名结果发送给收方，待收方验证。可见，数字签名是由发送方创建的。

2. 接收方收到数字签名的结果，其中包括数字签名、电子原文，即待验证的数据。

接收方进行签名验证，其验证过程是：接收方首先用发送方公钥解密数字签名，导出数字摘要，并对电子文件原文作同样哈希算法得一个新的数字摘要，将两个摘要值进行结果比较，相同签名得到验证，否则无效。

9.4.3 同步练习

1. 电子商务中的数字签名通常利用__(1)__加密方法实现，其中发送者签名使用的密钥为发送者的__(2)__。
2. 数字签名技术的主要功能是：__(1)__、__(2)__、防止交易中的抵赖发生。
3. 非对称密钥加密系统，又称__(1)__。其特点是加密和解密使用不同的密钥。非对称密钥加密的典型算法是__(2)__。

9.4.4 同步练习参考答案

1. (1)公开密钥 (2)私钥
2. (1)保证信息传输过程中的完整性 (2)发送者的身份认证
3. (1)公钥和私钥系统 (2)RSA

9.5 服 务 机 制

9.5.1 考点辅导

9.5.1.1 服务供应商、供应商漫游服务

Internet 是当今世界最大的、开放性的计算机互联网。经由 Internet 传递的信息要被路由器选择通过一个或多个主干网络，这些主干网络通常都是由大的 Internet 服务提供商 ISP(Internet Service Provider)所拥有。Internet 服务提供商提供了 Internet 底层结构。Internet 服务提供商负责 Internet 的日常维护和运行。当前，Internet 服务提供商提供的服务包括：互联、电子邮件、Web 页面、DNS、文件服务器、内容缓存等。

随着计算机技术的突飞猛进和 Internet 在全球的普及，新型电信服务——增值服务发展迅速。终端用户需求的激增刺激了增值服务业务的快速发展。目前电信行业的发展正在呈现两大趋势，首先是以个性化、差异化为特征的市场细分。这使得很多电信增值服务正开始以客户为中心，以量身定做的解决方案协助用户将复杂的问题简单化。其次，通信与 IT 走向融合的趋势已经势不可挡。一方面，通信技术与 IT 技术的融合是未来发展的主流方向，“通信-网络”的模式成为电信行业发展的风向标；另一方面，企业对通信服务和 IT 服务的需求也逐步统一和融合。可见，面对这一机遇与挑战，服务供应商必须提供更加强大和全面的技术水平和服务支持。

与 ISP 进行紧密合作的服务供应商(Service Provider，SP)也随之出现，为广大用户提供各式各样的增值服务，如新浪、搜狐、网易等。在互联网市场价值链中，SP 是不可缺少的

一环。而好的内容和应用则是启动市场的关键。SP 作为移动互联网服务提供商，是创业计划实施过程中的重要市场主体，他们的工作决定着用户的满意度。

同时，为了提高服务的全面性、消除地域的影响，各大 ISP 出尽奇招，提供了互联漫游的接入服务，使得用户即使在外地出差或旅游、甚至在路途上，也可以使用现有的网络接入账号以及密码，通过移动通信的方式进入互联网，而无需交付额外的长途费用。

9.5.1.2　拨号 IP 连接、CATV 连接

为了享受 ISP 所提供的服务，首先要做的是接入 Internet。接入互联网有多种方式，最普通的是拨号 IP 连接。所谓拨号 IP 连接，就是利用支持点对点协议(简称 PPP 方式)的软件，通过 Modem 和电话线在用户的计算机和 ISP 的设备之间建立一个完全的 Internet 连接，用户的计算机借助于 ISP 的设备直接连接到 Internet 上。

Modem 是一个数字信号与模拟信号之间的转换设备。在使用 Modem 接入网络时，因为要进行数字信号与模拟信号之间的转换，所以网络连接速度较低，而且性能较差。目前广泛使用的 56K Modem 的下行速率可以达到 56 Kb/s，而上行速率只有 33.6Kb/s。常见的 Modem 一般分为独立外置式和插卡内置式两种。外置式 Modem 通过 RS-232 电缆连接到计算机的一个串口上，而内置式一般使用 ISA 和 PCI 两种接口类型之一。

然而，一系列新的 Internet 服务，包括提供音频、视频流，视频点播以及其他大量网上服务，普通的拨号 IP 接入已经不能满足用户的需求。于是，人们开始竞相研究各种 Internet 宽带接入技术。比如 ISDN(综合业务数字网，俗称“一线通”)， ADSL(非对称数字用户线路)，ATM(帧中继)等，当然还有 CATV(有线电视)宽带接入。CATV 宽带接入的上行带宽可达 10Mb/s，下行带宽可达 35Mb/s，如此传输速率无疑是非常诱人的。

CATV 网是采用同轴电缆构成的，它的带宽很容易可以做到 800Mb/s，就现在的带宽需求而言，CATV 网的最后“一公里”是畅通的。当然，由于 CATV 网当初是用于广播式的电视传播，也就是说，它是单向的，所以要用于计算机网络时，必须对现有的网络前端和用户端进行改造，使之具有双向传输功能。

改造 CATV 网的技术方案很多，但目前使用较广泛的是光纤同轴混合网(HFC)。HFC 首先由贝尔实验室提出，它是基于传统的 CATV 网发展起来的一种新型宽带用户接入网。HFC 网的主干部分采用光纤，光节点到配线盒使用同轴电缆，配线盒到用户端使用分配型同轴引入线。HFC 实现双向传输的方式是在其光纤系统中采用空间分割法，分别用两根光纤传送上行和下行信号，而在同轴电缆中采用频率分割法。HFC 技术将数字信号调制成 QAM 信号，并以频分复用方式把语音信号、数据信号、按需视频点播、模拟有线电视信号综合在一起，再调制到激光器上，以模拟方式在光缆和同轴电缆系统中传输，在接收端通过解调恢复为原来的信号。

9.5.1.3　IP 电话

IP 电话作为传统公用电话的替代，一出现就以低廉的价格受到广大用户和通信厂商的关注。目前，已经进入到 IP 电话的实用化时代。

传统公用电话网采用面向连接的、基于 64Kb/s 信道的电路交换方式，通过信令来控制连接。这种方式的优点是服务质量有保障，控制相对简单。而 IP 电话技术是基于分组交换

网络的，通过 TCP/IP 协议在分组交换网上实时传送语音信息。

IP 电话采用了压缩编码及统计复用等技术，与 PSTN 语音通信相比，提高了传输线路利用率，节省了网络的带宽，从而降低了通信成本，并且能方便地开展增值的多媒体应用。IP 电话是网络通信技术、VoIP 技术发展进步的产物。

根据用户终端的不同，可以将 IP 电话技术应用分为三种方式：

(1) PC to PC

1995 年，VocalTec 公司开发出通过互联网打长途电话的软件 Internet Phone，从而将 IP 电话技术实用化。通话双方的计算机必须安装相同的网络通话软件，必须上网并登录到指定的网络服务器上，利用声卡和话筒进行通话。显然，这种方式所使用的方法复杂，不利于推广使用。

(2) PC to Phone (Phone to PC)

PC to Phone 的应用主叫方仍是计算机。在计算机上必须安装相应的网络通话软件，例如 Net2Phone。通话时，主叫方上网并登录到与被叫方电话网连接的 IP 电话网关上，通过网关将呼叫转接到被叫电话上。Phone to PC 的业务过程与 PC to Phone 相反，它实现了电话到计算机的直接通话，主要应用于建立新型的客户呼叫中心(也称为 Call Center)。这种方式比 PC to PC 方式在使用上更为简单，但是应用的领域却较为狭窄。

(3) Phone to Phone

主被叫双方均使用普通话机，通话时主叫方连接到 IP 电话网关，通过 IP 网络连接到与被叫方电话网相连的 IP 电话网关，再将呼叫转接到被叫电话上。Phone to Phone 的通话过程与传统电话没有区别，并且可以提供新颖的增值业务，正因为如此，以 Phone to Phone 为主的 IP 电话业务得到了迅猛的发展，使得 IP 电话不再是网络爱好者的专宠，而真正能够进入寻常百姓家。IP 电话技术的出现并迅速发展，预示着当今电信网络的基础结构正在经历着从传统电路交换向数据包交换的转变，从而将形成一个以数据包交换为基础提供多种综合业务的统一电信网络。

在传统的语音通信过程中，模拟语音经采样、量化、编码成为 64Kb/s 的数字信号，然后数字信号通过由长途和本地交换机所构成的电路交换网络传送。通话过程中主、被叫双方各自独占一条 64K 的带宽。由于通话过程中，大量的时间处于单方通话或静音状态，因此带宽的独占导致了资源的浪费。

在 IP 电话中，64Kb/s 的语音信号经网关转换成分组语音数据，通过 IP 网络传送到对方网关，再还原成 64Kb/s 的语音信号。IP 电话技术采用 IP 网络完成语音的透明传输，实现了长途中继的复用，并且采用先进的语音压缩算法，大大提高了长途中继的利用效率。通话过程中的呼叫控制是由 IP 电话网关完成的。

在 IP 电话技术的应用过程中涉及到一些关键技术：

(1) 网络传输技术，主要包括基于 TCP/IP 协议的 IP 网络实时传输和服务质量保障技术，如实时传输协议 RTP、实时传输控制协议 RTCP 以及资源预留协议 RSVP 等。

(2) 语音编码技术，如 G.711、G.723、G.728、G.729 等。

(3) 信令技术，主要包括 PSTN 侧信令，如 1 号信令、7 号信令等，以及 IP 网内的信令技术，如 H.323 协议等。

(4) 计费，主要有 RADIUS 协议等实时认证计费技术。

IP 电话技术在短短的几年时间里得到了飞速地发展，但是相应的协议规范仍在不断地完善着。例如，在互通性方面，H.225 ANNEX G 的出现为实现各厂家产品的互通迈出了实质性的一步；在呼叫信令协议方面，H.323 目前成为了主流的标准，但是随着网络规模的扩大，MGCP 系列和 SIP 系列也得到了充分地发展。

9.5.1.4　因特网广播和组播

因特网广播是指通过因特网在电脑上收听/收看网络电视或电台广播。因特网广播的实现主要依赖于 IP 组播技术。

IP 组播技术是优化带宽的重要手段，它适用于多点到多点或一点到多点的数据传输业务。利用 IP 组播技术可以使得网络中的数据包在数据分布树的分叉处进行复制，而不是由数据源节点多次重复地发送相同的数据包。

IP 组播技术利用的是 D 类 IP 地址，组播地址的范围为：224.0.0.0～239.255.255.255。将能够接收发往某个特定组播组地址数据的主机集合称为主机组(host group)。一个主机组可以跨越多个网络。主机组中的成员可以随时加入或离开主机组。主机组中主机的数量没有限制。

一些组播地址被 IAN 定义为保留地址，它们被当做永久主机组，这与 TCP、UDP 中的保留端口相似。需要注意的是：这些组播地址所代表的组是永久组，而它们的组成员却不是永久的。例如，224.0.0.1 代表“网络内的所有系统或主机”，224.0.0.2 代表“网络内的所有路由器”，224.0.0.9 用于路由协议 RIPv2，224.0.1.1 用于网络时间协议 NTP。

9.5.1.5　电子政务、电子商务

信息技术发展到今天，Internet 已经直接影响着我们的生活，信息网络正在成长为“第四媒体”，它也将成为人们获得信息和实现社会多种功能的主要载体。近年来，为提高我国的国际竞争优势，政府推出国家信息基础建设，并规划利用网络构建“电子化政府”或叫“电子政务”。

电子政务不仅能提高工作效率，推进政务公开和廉政建设，提高政府服务水平，而且它也是建立和完善社会主义市场经济，保障社会的公正和公平，增强国家的竞争力，应对经济全球化挑战的重大战略措施。

从世界范围来看，推进政府部门办公自动化、网络化、电子化，以及全面信息的共享，已是大势所趋。联合国经济社会事务部把推进发展中国家政府信息化作为近几年的重点，希望通过信息技术的应用改进政府组织，重组公共管理，最终实现办公自动化和信息资源的共享。在世界各国积极倡导的“信息高速公路”的五个应用领域中，“电子政务”被列为第一位，其他四个领域分别是电子商务、远程教育、远程医疗、电子娱乐，可以认为政府信息化是社会信息化的基础。

电子政务最重要的内涵是运用信息及通信技术打破行政机关的组织界限，构建一个电子化的虚拟机关，使得人们可以从不同的渠道取用政府的信息及服务，而不是传统的、要经过层层关卡书面审核的作业方式；而政府机关之间及政府与社会各界之间也是经由各种电子化渠道来进行相互间沟通，并依据人们的需求、人们可以使用的形式、人们要求的时间及地点，提供给人们各种不同的服务选择。进行电子政务的架构，可以从应用、服务以

及网络通道这三个层面上进行规划。

“信息高速公路”应用的另一个重要领域就是电子商务。电子商务就是利用当代计算机技术、网络通信技术、多媒体技术等技术实现、完成各种商务行为、活动。从狭义上说，电子商务就是电子贸易，主要指利用 Web 提供的手段在网上进行电子交易，包括通过 Internet 买卖产品和提供服务。从广义上说，电子商务还包括企业内部的商务活动，如生产、管理、财务以及企业间的商务活动。

2004 年 1 月 15 日 中国互联网络信息中心(CNNIC)在北京发布了《第十三次中国互联网发展状况统计报告》。报告中指出，截至 2003 年 12 月 31 日，中国网民总数已达到 7950 万，较(第十二次互联网统计报告)半年前增加了 1150 万；CN 下注册域名数量增长迅速，达到了 34 万，半年增长近 10 万；WWW 站点总数接近 60 万，半年内增长 12 万；国际出口带宽达到 27 216Mb/s，中国互联网业发展稳步前行。在日渐壮大的网络用户中，政府、企业的角色举足轻重。这样也促进了电子政务、电子商务的发展，从而构筑一个新的 Internet。

电子商务经历了 B2C→B2B→电子交易市场等不同的发展阶段，对于商业模式的探索已经初见端倪。那什么是 B2B、B2C 的商业模式呢？

B2C(企业对个人的电子商务)是人们最熟悉的一种商务类型，以至许多人错误地认为电子商务就只有这样一种模式。事实上，这缩小了电子商务的范围，错误地将电子商务与网上购物等同起来。近年来，随着 Internet 技术的兴起，出现了大量的网上商店，由于 Internet 提供了双向的交互通信，网上购物不仅成为了可能，而且成为了热门。由于这种模式节省了客户和企业双方的时间、空间，大大提高了交易的效率，节省了各类不必要的开支，因而，这类模式得到了人们的认同，获得了迅速地发展。

在电子商务中，公司也可以用电子形式将关键的商务处理过程连接起来，以形成虚拟企业，这被称作 B2B(企业间电子商务)模式。在这种环境中，很难区分哪家公司正在进行商务活动。一家公司在一台 PC 机或移动式电脑上按下一个键就有可能影响一家处于地球另一端的供货公司的业务活动。尽管眼下网上企业直接面向客户(B2C)的销售方式发展势头强劲，但为数众多的分析家认为企业间的商务活动更具潜力。一些电子商务的研究公司预计，企业间的商务活动将以三倍于企业与个人之间的商务活动速度发展。

9.5.1.6 电子数据交换

电子数据交换(Electronic Data Interchange，EDI)是一种在公司之间传输订单、发票等作业文件的电子化手段，是企业利用计算机进行商业合作的一种方法。EDI 是将贸易、银行、保险和海关等行业信息，采用一种国际公认的标准格式，通过计算机通信网络，实现各有关部门、公司与企业之间的数据交换与处理，并完成以贸易为中心的全部业务过程。

EDI 是 20 世纪 80 年代发展起来的一种新颖的电子化贸易工具，是计算机、通信和现代管理技术相结合的产物。国际标准化组织(ISO)将 EDI 描述成“将贸易(商业)或行政事务处理按照一个公认的标准变成结构化的事务处理或信息数据格式，从计算机到计算机的电子传输”。由于使用 EDI 可以减少甚至消除贸易过程中的纸面文件，因此 EDI 又被人们通俗地称为“无纸贸易”。

从上述 EDI 定义不难看出，EDI 包含了三个方面的内容，即计算机应用、通信网络和

数据标准化。其中计算机应用是 EDI 的条件，通信网络是 EDI 应用的基础，数据标准化是 EDI 的特征。这三方面相互衔接、相互依存，构成了 EDI 的基础框架。

最早把 EDI 带入 Internet 的是 E-mail，这样利用 ISP 的网络代替了传统的 EDI 所依赖的专有网络。但是，E-mail 方式的 EDI 存在着严重的安全、保密等问题。目前，Web EDI 方式被认为是 EDI 最好的实现方式。Web EDI 允许企业只需要通过标准化的浏览器软件和广泛应用的 Internet 去执行 EDI 交换——Web 是 EDI 的消息接口。由于 Internet 的通用性和使用成本的低廉，因此使用 Web EDI 的固定成本也比较低廉。Web EDI 是在原来 EDI 的基础上改造而来的，因此企业应用这样方式只需对现行系统做很小的改动，就可以快速地扩展成为 Web EDI 应用系统。

9.5.1.7　移动通信

从 20 世纪 80 年代起，移动通信技术获得了很大的发展，从传统的单基站大功率系统到蜂窝移动系统、卫星移动系统；从本地覆盖到区域、全国覆盖，并实现了国内、国际漫游；从提供语音业务到提供包括数据的综合业务；从模拟移动通信系统到数字移动通信系统等，今后移动通信技术还会进一步快速发展。随着第三代移动通信技术的商用和移动网与互联网的融合，全球正在向移动信息时代迈进。

1. 蜂窝移动通信

蜂窝移动通信是采用蜂窝无线组网方式，在终端和网络设备之间通过无线通道连接起来，进而实现用户在活动中可以相互通信。它的主要特征是终端的移动性，并且具有越区切换和跨本地网自动漫游功能。蜂窝移动通信业务是指由基站子系统和移动交互子系统等设备组成蜂窝移动通信网提供的语音、数据、视频等业务。

目前，蜂窝移动通信的业务包括：900/1800 MHz GSM 第二代数字蜂窝移动通信业务、800MHz CDMA 第二代数字蜂窝移动通信业务、第三代数字蜂窝移动通信业务。

2. GSM 第二代数字蜂窝移动通信业务

900/1800 MHz GSM 第二代数字蜂窝移动通信(简称 GSM 移动通信)业务是指使用工作在 900/1800 MHz 频段的 GSM 移动通信网络提供的语音和数据业务。GSM 移动通信的无线接口采用 TDMA 技术，核心网络移动性管理协议采用 MAP 协议。

900/1800 MHz GSM 第二代数字蜂窝移动通信业务主要包括以下几种类型：

- 端到端的双向语音业务。
- 移动消息业务。
- 移动承载业务以及数据业务。
- 移动补充业务，如主叫号码显示、呼叫前转业务等。
- 国内、国际漫游业务。

3. CDMA 第二代数字蜂窝移动通信业务

800MHz CDMA 第二代数字蜂窝移动通信(简称 CDMA 移动通信)业务是指利用工作在 800MHz 频段上的 CDMA 移动通信网络提供的语音和数据业务。CDMA 移动通信的无线接口采用窄带码分多址 CDMA 技术，核心网络移动性管理协议采用 IS-41 协议。

800MHz CDMA 第二代数字蜂窝移动通信业务与 900/1800 MHz GSM 的主要业务类型

相同。

4. 第三代数字蜂窝移动通信业务

第三代数字蜂窝移动通信(简称 3G 移动通信)业务是指利用第三代数字移动通信网络提供的语音、数据、视频等业务。

第三代数字蜂窝移动通信业务的主要特征是可以提供移动宽带多媒体业务，其中高速移动环境下支持 144Kb/s 的带宽速率，步行和慢速移动环境下支持 384Kb/s 的带宽速率，室内环境下支持高达 2Mb/s 的带宽速率，同时还能保证高可靠的服务质量(QoS)。第三代数字蜂窝移动通信业务包括了第二代数字蜂窝移动通信可以提供的所有业务类型以及移动多媒体业务。

9.5.1.8 EZweb

EZweb 是日本现有的手机上网服务之一，是目前世界上最广泛、最成功的 WAP 服务。

1999 年 10 月日本第二电信(DDI)和日本移动通信(IDO)及 KDD 三家公司合并，成为日本第二大移动运营商 KDDI。KDDI 于 2000 年 6 月 30 日，发表了面向移动电话的因特网业务计划，这个业务被称为“EZweb”。 EZweb 利用公共数据交换网构建服务平台。EZweb 的极限数据传输速率达到 14.4Kb/s。EZweb 采用的是 CDMA One(Qudcom 公司的 CDMA 格式)和 PDC(日本数字通信标准)格式。

9.5.1.9 数据中心、主机服务提供者、应用服务提供商

互联网市场历经了 ISP 的风靡和.com 狂飙的席卷之后，一个“新的”名词、一种“新的”服务方式——互联网数据中心(IDC，Internet Data Center)正在兴起，并迅速火爆起来。其实，数据中心并不是一个新生事物，它在大型主机时代就已经出现，当时是为了通过托管、外包或集中方式向企业提供大型主机的管理维护，以达到专业化管理和降低运行成本的目的而出现的。虽然 IDC 还没有一个权威的定义，但它比传统的数据中心有着更深层次的内涵：它是伴随着因特网不断增长的需求而发展起来的，为 ICP、企业、媒体和各类网站提供大规模、高质量、安全可靠的专业化服务器托管、空间租用、网络批发带宽等业务。

互联网数据中心是入驻企业、商户或网站服务器托管的场所，是各种模式电子商务赖以安全运作的基础设施，也是支持企业及其商业联盟实施价值链管理的平台。这也就是为什么人们把它比喻成“数码大厦”的原因。

互联网数据中心所提供的一些业务中，最为普遍的就是主机托管业务，即主机服务业务。通过购买 IDC 主机服务业务，企业或政府单位无需建立自己的专门机房，铺设昂贵的通信线路，也无需高薪聘请网络工程师——可以由 IDC 内的深资的网络工程师为客户提供全天候、全方位、高质量的技术服务。

近年来，一些企业基于互联网数据中心得天独厚的资源优势，专门提供计算机应用服务，这些应用在订购的基础上通过网络提供给用户。我们将这些企业称为 ASP(Application Service Provider，应用服务提供商)。ASP 业务是指配置、租赁和管理应用服务的解决方案，为企业、个人提供服务的专业化服务公司。通俗地说，ASP 是一种业务租赁模式，企业用户可以直接租用 ASP 的计算机及软件系统进行自己的业务管理，从而节省一大笔将用于 IT 产品购买和运行的资金。

ASP 是一场新的革命。它以应用为业务核心，出售应用访问，进行集中管理，可以为多个客户提供服务。ASP 和传统资源外包商之间的本质区别在于：ASP 是在一个中心地点而不是在客户所在地，管理应用程序及其部件；ASP 是通过标准的 Web 接口来实现在网上的存取；ASP 可根据需要进行扩缩，可集中进行升级和维护。

目前，传统的各项 Internet 增值服务已不再适应电子商务的发展，同时，网站泡沫已经破灭，ASP 模式将会成为电子商务的新一轮浪潮。国内部分有实力的 IT 公司已经开始涉足 ASP 的小部分业务，如：企业财务管理的 ASP、客户关系管理的 ASP、ERP 领域的 ASP、网上办公领域的 ASP、金融领域的 ASP 等。

9.5.2　典型例题分析

例　阅读以下说明，回答问题。

【说明】

网络系统对访问速度的高要求导致了对带宽的高要求；电子商务的发展使得网络系统稳定性对于企业越来越重要；网络系统自身的快速发展要求能够方便地扩展网络环境；网络系统的日趋复杂使得网站管理难度更高，系统维护所需要的人力成本也在升高。因此，许多公司开始寻求资源外包这种经济可靠的网络服务方式，一批专门提供网络资源外包以及专业网络服务的 Internet 数据中心(IDC)也应运而生。

互联网数据中心有两个非常重要的特征：IDC 不是数据存储的中心，而是数据流通的中心，它应该出现在 Internet 巨大的网络中数据交换最集中的地方；互联网数据中心 IDC 应具备十分丰富的带宽资源、安全可靠的机房设施、高水平的网络管理、十分完备的增值服务。

【问题】

图 9.13 描述了 IDC 数据中心的一般网络结构以及基本构成区域。根据此 IDC 数据中心完成下面的问题。

1.　为做电子商务的客户选择数据中心所提供服务的一个区域——需要考虑其日后的业务拓展。

2.　简述此 IDC 数据中心的网络层次结构，并说明一般主机服务(主机托管)业务应选择的网络层次。

3.　目前，为了评价 IDC 所提供的各种业务，业界出现了 SLA 评估方法。简述何为 SLA?

分析：安全性是 IDC 用户特别是电子商务用户最为关注的问题，也是 IDC 建设中的关键，它包括物理空间的安全控制及网络的安全控制——应有完整的安全策略控制体系以实现 IDC 安全控制。

IDC 的关键技术有："交易状态维系"(Stateful)的功能，可保证电子商务的无损失交易；基于硬件处理可实现线速的安全控制；提供 DoS 服务以防止对于网络的恶意进攻；提供 SSH 功能可对采取远端管理的 Telnet 方式进行加密以保证管理的安全性；内容识别(Content Aware)网络——现今的 IDC 具有内容的识别能力是其主要的技术特征，可提供多种技术保证基于内容的有效交换；"Cookie"锁定技术保证在进行电子商务中避免"丢失购物车(Lost Shopping Cart)"的事件发生；动态内容复制功能可根据用户访问量的增加自动启动复制功

能；智能化高速缓存(Caching)加快了对客户请求的响应速度；智能化负载均衡更加合理地将网络数据流分配到各种各样的后台服务器上；防火墙的负载均衡功能实现了防火墙功能的备份与负载均衡，提高安全性及吞吐能力。

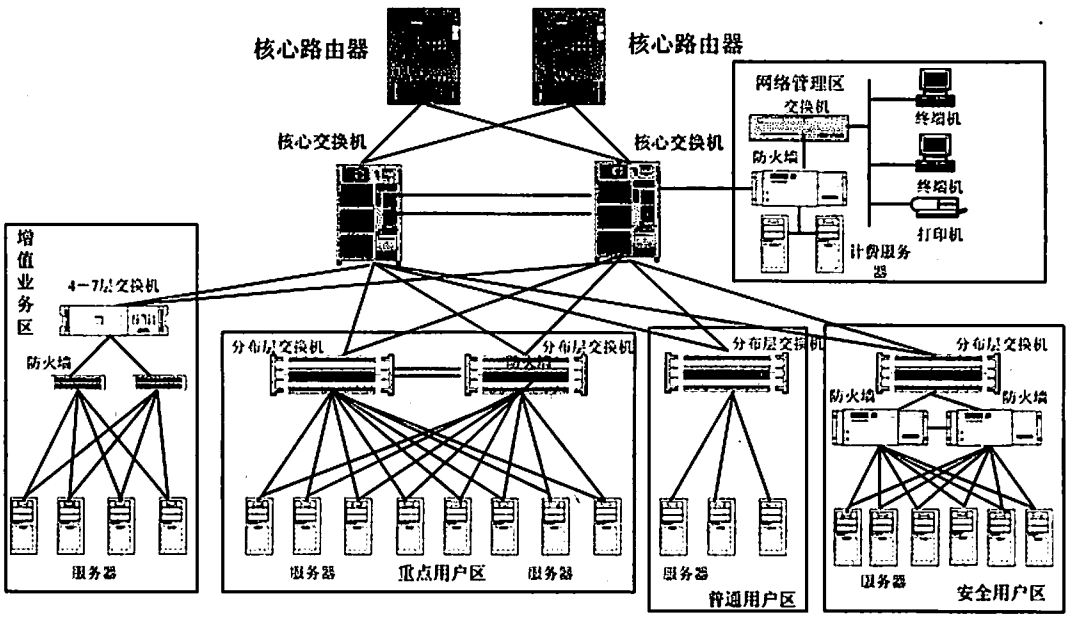


图 9.13 IDC 网络拓扑图

图 9.13 的 IDC 方案中，采用了层次化的设计，为 IDC 的日后扩展奠定基础。此 IDC 具体可分为 Internet 互联层、核心层、分布层，并且这些网络层次上的设备都应该采用模块化设计，可根据 IDC 网络的发展进行灵活扩展。

对于此 IDC 方案采用的路由协议，可以这样：连接 Internet 可以采用 BGP4 协议、内部 IGP 采用 OSPF/IS-IS、边缘采用默认路由。使得整个 IDC 网络具有极强的路由扩展能力。

功能的可扩展性是 IDC 随着发展提供增值业务的基础。实现负载均衡、动态内容复制、MPLS VPN、Private VLAN 等功能，为 IDC 增值业务的扩展提供了基础。而对于 IDC 的一般托管业务，只需要向用户提供与 Internet 连接以及提供独立安全的场地就可以达到要求。

在 IDC 推出新的价格模式的同时，为了保证客户所得到的服务品质，业界提出了“服务品质协议(SLA，Service Level Agreement)”，以确保网络的速度和服务。除“网络联通率”与“电源持续供应”两个原有指标外，IDC 数据中心尝试在“服务品质协议”中对“网络速度”做出承诺。

SLA 不仅明确了违约方的经济惩罚性条款，而且有助于用户对服务商提供具体服务的能力、可靠性和响应速度进行充分正确的评估和监督。为保障服务品质，除了以往的托管服务之外，IDC 的服务内容还可以包括：网络/系统/数据库安全检测、安全漏洞修补服务、24×7 实时入侵监控服务、网络入侵紧急响应服务。而在负载均衡服务中，采用先进的 4 到 7 层交换技术，支持所有基于 TCP 和 UDP 的业务。

答案：

1. 考虑到安全性以及业务的弹性，做电子商务的客户应该选择 IDC 数据中心的“增

值业务区”。

2. 此 IDC 方案采用了层次化的设计：Internet 互联层、核心层、分布层、接入层。对于 IDC 的一般托管业务的用户，其主机(服务器)直接从网络接入层接入就可以达到要求。

3. SLA 是“服务品质协议”的简称，是一种由 IDC 服务提供商与用户签署的法律文件，是市场走向规范化的表现之一。SLA 是服务提供商实力的重要体现，是用户选择 IDC 的主要参考标准。

9.5.3 同步练习

1. 电子商务采用层次化的体系结构，支付型电子商务体系结构的四个层次从下至上依次为__(1)__、__(2)__、__(3)__和__(4)__。在电子商务活动中，消费者与银行之间的资金转移通常要用到证书，证书的发放单位是__(5)__。

2. 最后“一公里”的宽带接入方式除了有 ADSL 外，还有 CATV(有线电视)宽带接入。CATV 宽带接入的上行带宽可达__(1)__，下行带宽可达__(2)__。CATV 的改造方案中，用得最为普遍的是__(3)__技术。

3. EDI 包含了三个方面的内容，即__(1)__、__(2)__和__(3)__。

9.5.4 同步练习参考答案

1. (1)网络基础平台　(2)安全保障　(3)支付体系　(4)业务系统
   (5)安全认证中心(CA)
2. (1)10Mb/s　(2)35Mb/s　(3)HFC
3. (1)计算机应用　(2)通信　(3)网络和数据标准化

9.6 本 章 小 结

本章主要要求考生掌握 TCP/IP 协议族的基本概念以及其所提供的相关应用服务、最新的交换技术(Web 交换)、电子身份验证以及 Internet 上的所使用的服务机制。本章内容包括 IP 地址的分配、子网掩码以及 IPv6 的机制和传输技术；TCP/IP 协议栈的 DNS、SMTP/POP、NNTP、HTTP 服务等；基于智能内容识别的 Web 交换；电子身份验证以及 Internet 服务机制的基础知识。

对 TCP/IP 协议栈的学习关键要建立整体观念，首先要参考 ISO 的网络开放模型(OSI)来熟悉各个层次的协议。本章的每小节中组织了大量的针对水平考试的典型例题分析和同步训练，这些题目涵盖了大纲规定的知识要点。

第 10 章　网络新技术

大纲要求：

- 光纤网　ATM-PDS、STM-PDS，无源光网 PON(APON、EPON)。
- 无线网　移动电话系统(WLL、WCDMA、CMDA2000、TD-SCDMA)，高速固定无线接入(FWA)，802.11a、802.11b、802.11g，微波接入(MMDS、LMDS)，卫星接入，蓝牙接入。
- 主干网　IP over SONET/SDH，IP over Optical，IP over DWDM。
- 通信服务。
- 网络管理　基于 TMN 的网络管理，基于 CORBA 的网络管理。
- 网格计算。

10.1　光　纤　网

10.1.1　考点辅导

10.1.1.1　无源光网络的概念

无源光网络(Passive Optical Network，PON)是指在 OLT(光线路终端)和 ONU(光网络单元)之间的光分配网络(ODN)没有任何有源电子设备。

PON(无源光网络)技术是一种点对多点的光纤传输和接入技术，下行采用广播方式、上行采用时分多址方式，可以灵活地组成树形、星形、总线形等拓扑结构，在光分支点不需要节点设备，只需要安装一个简单的光分支器即可，因此具有节省光缆资源、带宽资源共享、节省机房投资、设备安全性高、建网速度快、综合建网成本低等优点。

PON 包括 ATM-PON(APON，即基于 ATM 的无源光网络)和 Ethernet-PON(EPON，即基于以太网的无源光网络)两种。

10.1.1.2　ATM-PDS 和 STM-PDS

无源双星组网形式(PDS，Passive Double Star)是 PON 的一种典型的组网形式，这种组网形式使 PON 的特点得到了恰到好处的体现。它适合于距离 OLT 较远的邻近周围均匀分散的用户服务区，例如，农村乡镇的用户接入。有两种 PDS 技术实现形式：ATM-PDS (Asynchronous Transfer Mode -Passive Double Star)和 STM-PDS(Synchronous Transfer Mode - Passive Double Star)。ATM-PDS 能够为服务区内的所有用户提供最大 156Mb/s 传输率的服务。这样的系统可以满足多媒体服务的要求。然而，还是有一些其他问题尚未很好的解决，例如，当前 ATM 相关的设备还是很昂贵。这样也就有了 STM-PDS 组网形式的存在。

10.1.1.3　无源光网络的优势

无源光网络(PON)是一种纯介质网络，避免了外部设备的电磁干扰和雷电影响，减少了线路和外部设备的故障率，提高了系统的可靠性，同时节省了维护成本，是电信维护部门长期期待的技术。无源光网络的优势具体体现在以下几方面：

- 无源光网络设备简单，安装维护费用低，投资相对也较小。
- 无源光网络设备组网灵活，拓扑结构可支持树型、星型、总线型、混合型、冗余型等网络拓扑结构。
- 安装方便，它有室内型和室外型。其室外型可直接挂在墙上，或放置于“H”杆上，无需租用或建造机房。而有源系统需进行光电、电光转换，设备制造费用高，要使用专门的场地和机房，远端供电问题不好解决，日常维护工作量大。
- 无源光网络适用于点对多点通信，仅利用无源分光器实现光功率的分配。
- 无源光网络是纯介质网络，彻底避免了电磁干扰和雷电影响，极适合在自然条件恶劣的地区使用。
- 从技术发展角度看，无源光网络扩容比较简单，不涉及设备改造，只需设备软件升级，硬件设备一次购买，长期使用，为光纤入户奠定了基础，使用户投资得到保证。

10.1.1.4　基于 ATM 的无源光网络

1. APON 技术简介

近年来，在接入网上使用 ATM 技术以提供视频广播、远程教育以及数据通信等多种业务的趋势越来越明显。在无源光网络上使用 ATM，不仅可以利用光纤的巨大带宽提供宽带服务，也可以利用 ATM 进行高效的业务管理。自 1993 年以来，许多国家都竞相开始研究 ATM-PON 技术及其应用，并认为 ATM-PON 是最有前途的、能以较低成本提供宽带接入的方案。

APON 技术发展得比较早，它还具有综合业务接入、QoS 服务质量保证等独有的特点，ITU-T 的 G.983 建议规范了 ATM-PON 的网络结构、基本组成和物理层接口，我国信息产业部也已制定了完善的 APON 技术标准。

ATM-PON 采用的是点到多点的无源光网络，主要由 OLT、ODN、ONU 组成，由无源光分路器件将 OLT 的光信号分到树形网络的各个 ONU。其应用包括 FTTH、FTTB/C、FTTCab 等多种配置结构。FTTB/C 和 FTTCab 网络结构只是在应用上略有区别，可以看成一类。FTTB/C/Cab 可以提供 PSTN、ISDN 业务以及其他对称或非对称的宽带业务。

FTTH 应用提供的业务大致同上，另外，FTTH 可以考虑使用户内置 ONU，使 ONU 的工作环境得以改善，再加上网络全部为光纤，使得维护工作量减少、成本降低。对于网络将来可能的带宽或业务升级，ONU 可不作改动。

根据 G.983 规范，在 ATM 无源光网络中，OLT 最多可寻址 64 个 ONU，PON 所支持的虚通路(VP)数为 4096，PON 寻址可以使用 ATM 信元头中的 12 位 VP 域。由于 OLT 具有 VP 交叉互联功能，所以局端 VB5 接口的 VPI 和 PON 上的 VPI(OLT 到 ONU)是不同的。限制 VP 数为 4096，使 ONU 的地址表不会很大，同时又保证了高效利用 PON 资源。

APON 的业务开发是分阶段实施的，第一步主要是 VP 专线业务。相对普通专线业务，

APON 提供的 VP 专线业务设备成本低、体积小、省电、系统可靠稳定、性能价格比有一定优势。第二步实现一次群和二次群电路仿真业务，提供企业内部网的连接和企业电话及数据业务。第三步实现以太网接口，提供互联网上网业务和 VLAN 业务。以后再逐步扩展至其他业务，成为名副其实的全业务接入网系统。

APON 采用基于信元的传输系统，允许接入网中的多个用户共享整个带宽。这种复用的方式，能更加有效地利用网络资源。

2. APON 技术的应用前景

目前许多国家都在实验 PON 接入网，如日本的 π 系统采用的是 STM 的 PON 技术，无源双星的网络结构。其 ONU 配置灵活，可以为单个用户提供 1.5Mb/s 的接入速率。欧洲关于 PON 的研究有 ACTSAC094Expert 项目、ACTSAC022Bonaparte 项目和 RACEIIR2024BAF 项目等。其中 Bonaparte(在现实电信环境下使用 ATM-PON 接入设备的宽带光网络)在 4 个国家分别进行用户实验，并根据用户的实际需求提供远程医疗、远程教学等多媒体宽带业务。在 Bonaparte 中使用的 ATM-PON 连接 32 个终端，可以支持最大距离为 10 公里的 81 个用户。接入系统总的传输容量为上行和下行各 622Mb/s，每个用户使用的带宽可以从 64Kb/s 到 155Mb/s 灵活划分。

ATM-PON 支持 ISDN 及 B-ISDN 业务的带宽需求，可以满足各类电信业务的全业务网(FSN)的共同要求，ATM-PON 代表了宽带接入技术的最新发展方向，目前在英国、德国等已有实际应用，它被认为是实现 FTTC 和 FTTH 的一种较好方法，其优点是可以节省光纤和光设备的费用，并实现宽带数据业务与 CATV 业务的共网传送。

APON 能否大量应用的一个重要因素是价格问题。目前第一代的实际 APON 产品的业务供给能力有限，成本过高，其市场前景由于 ATM 在全球范围内的受挫而不确定，但其技术优势是明显的。特别是综合考虑运行维护成本，在新建地区、高度竞争的地区或需要替代旧铜缆系统的地区使用 PON 系统，无论是 FTTC，还是 FTTB 方式都是一种有远见的选择。在未来几年，能否将性能价格比改进到市场能够接受的水平是 APON 技术生存和发展的关键。

10.1.1.5 基于以太网的无源光网络

随着 Internet 的高速发展，用户对网络带宽的需求不断的提高，传统的接入网已经成为整个网络中的瓶颈，以新的宽带接入技术取而代之已成为目前研究的热点。正是在这种背景下，IEEE 于 2000 年底成立了 EFM 工作组(Ethernet in the First Mile Study Group)，试图引入一种新的接入技术标准——Ethernet PON(Ethernet over PON，EPON)。顾名思义，EPON 是利用 PON(无源光网络)的拓扑结构实现以太网的接入。

1. EPON 与 APON 的比较

ITU-T 已经制定了 APON 技术的 G.983 建议。但是 APON 有两个问题：一是传输速率不够高，下行为 622 Mb/s 或 155 Mb/s，上行为 155 Mb/s，带宽被 16~32 个 ONU 所分享，每个 ONU 只能得到 5Mb/s~20Mb/s 的速率的带宽；另一个更主要的问题是，与以太网设备相比，ATM 交换机和 ATM 终端设备相当昂贵。而且，现在因特网工作于 TCP/IP 协议，用户终端设备都是 IP 设备，采用 ATM 技术必须将 IP 包拆分后重新封装为 ATM 信元，这就大大增加了网络的开销，造成网络资源的浪费。

而 EPON 融合了 PON 和以太网产品的优点，形成了许多独有的优势。EPON 系统能够提供高达 1Gb/s 的上下行带宽，这一带宽能够适应现在及将来 10 年内用户对带宽的需求。由于 EPON 采用复用技术，支持更多的用户，每个用户可以享受到更大的带宽。EPON 系统不采用昂贵的 ATM 设备和 SONET 设备，能与现有的以太网相兼容，大大简化了系统结构，成本低，易于升级。由于无源光器件有很长的寿命，户外线路的维护费用大为减少。标准的以太网接口可以利用低廉的以太网络设备。PON 结构本身就决定了网络的可升级性比较强，只要更换终端设备，就可以使网络升级到 10 Gb/s 或者更高速率。EPON 不仅能综合现有的有线电视、数据和语音业务，还能兼容未来业务，例如：数字电视、VoIP、电视会议和 VOD 等，实现综合业务接入。

2. EPON 的系统结构

EPON 由光线路终端(OLT)、光合/分路器和光网络单元(ONU)组成，采用树形拓扑结构。

OLT 放置在中心局端，分配和控制信道的连接，并有实时监控、管理及维护功能。ONU 放置在用户端，OLT 与 ONU 之间通过无源光合/分路器连接。

EPON 使用波分复用(WDM)技术，同时处理双向信号传输，上、下行信号分别用不同的波长，并在同一根光纤中传送。EPON 只在 IEEE 802.3 的以太数据帧格式上做必要的改动，如在以太帧中加入时戳(Time Stamp)、PON-ID 等内容。下行采用纯广播的方式，注册后，OLT 为已注册的 ONU 分配 PON-ID，由各个 ONU 监测到达帧的 PON-ID，以决定是否接收该帧，如果该帧所含的 PON-ID 和自己的 PON-ID 相同，则接收该帧；反之则丢弃。上行采用时分多址接入(TDMA)技术。此外 EPON 还需通过已定义的接口与电信管理网相连，进行配置管理、性能管理、故障管理、安全管理及计费管理，完成操作维护管理(OAM)功能。

3. EPON 的关键技术

EPON 的关键技术主要包括上行信道复用技术、测距和时延补偿技术、光器件技术以及突发信号的快速同步技术。

(1) 上行信道复用技术

可以说上行的复用技术是 EPON 技术的核心。从目前的研究来看，大多数方案都使用了 DWDM+TDMA 的复用方法。DWDM 的使用是发展的趋势，但主要取决于光器件。因此，主要讨论的焦点将是 TDMA 的实现方法，即如何使用 TDMA 的方法使上行信道的带宽利用率、时延和时延抖动等指标达到要求。其中，上行带宽的分配方法、ONU 发送窗口固定还是可变、最大的 ONU 发送窗口应为多大、ONU 发送窗口的间隔、以太网帧是否切割等问题都有待于研究和确定。

(2) 测距和时延补偿技术

由于光纤信道时延较大的特点，ONU 与 OLT 之间的距离将会影响到上行信道的复用，如果能够准确地测量各个 ONU 到 OLT 的距离并能精确地调整 ONU 的发送时延，则可以减小 ONU 发送窗口间的间隔，从而提高上行信道的利用率并减小时延。另外，测距过程应充分考虑整个 EPON 的配置情况。例如，系统在工作中加入新的 ONU，此时对它的测距不应对其他 ONU 有太大的影响。

(3) 光器件

由于 EPON 上行信道是所有 ONU 分时复用的，每个 ONU 只能在指定的时间窗口内发送数据。因此，EPON 上行信道中使用的是突发信号，这就要求在 ONU 和 OLT 中使用支持突发信号的光器件。现有的大部分光器件还不能满足这一要求，少数突发模式的光器件也只能工作在 155Mb/s 的速率上，而且价格昂贵。可以说，这是 EPON 技术面临的一大问题，但是，目前已有厂商正在研制满足 EPON 要求的光器件，相信随着 EPON 标准的制定，会有更多的产品出现。

(4) 突发信号的快速同步

由于 OLT 接收到的信号为突发信号，因此 OLT 必须在很短的时间内实现相位的同步，进而接收数据。这一技术与 APON 中使用的类似，因此可以借鉴 APON 的经验。

除此之外，下行信道安全性、如何实现 QoS、如何实现 VLAN 和网络管理等也是影响 EPON 应用前景的问题，必须加以考虑。

4. EPON 的未来

EPON 还处于商业开发的起始阶段。尽管 APON 在市场上略微领先，但目前的趋势是数据业务快速增长和快速以太网、G 比特以太网的地位提高，都倾向于 EPON。

10.1.2 典型例题分析

例 1 简述两种实现 FTTH 的技术，并对这两种技术进行比较。

分析：APON 和 EPON 是实现 FTTH 的两种技术。详见 10.1.1.4 节和 10.1.1.5 节。

答案：略。

例 2 列举影响 EPON 的关键技术。

分析：详见 10.1.1.5 节。

答案：上行信道复用技术、测距和时延补偿技术、光器件的发展、突发信号的快速同步、下行信道安全性、如何实现 QoS、如何实现 VLAN 和网络管理等。

10.1.3 同步练习

1. 简述无源光网络的优势。
2. 什么是 PON?
3. 什么是 PDS?

10.1.4 同步练习参考答案

1. 详见 10.1.1.3 节。

2. PON(无源光网络)技术是一种点对多点的光纤传输和接入技术，下行采用广播方式、上行采用时分多址方式，可以灵活地组成树型、星型、总线型等拓扑结构。

3. 无源双星组网形式(PDS，Passive Double Star)是 PON 的一种典型的组网形式，这种组网形式使 PON 的特点得到了恰到好处的体现。ATM-PDS(Asynchronous Transfer Mode - Passive Double Star)和 STM-PDS(Synchronous Transfer Mode - Passive Double Star)是 PDS 技

术的两种实现方式。

10.2 无 线 网

10.2.1 考点辅导

10.2.1.1 移动电话系统(WLL、WCDMA、CMDA2000、TD-SCDMA)

1. WLL(Wireless Local Loop)

无线本地环路(WLL)是通过无线信号取代电缆线，连接用户和公共交换电话网络(PSTN)的一种技术。WLL 系统包括无线接入系统、专用固定无线接入以及固定蜂窝系统。在某些情况下，WLL 又称为环内无线(RITL)接入或固定无线接入(FRA)。WLL 的带宽使用率高于电缆环路。对于不具备线路架构条件的地方，如某些偏远地区或发展中国家而言，WLL 提供了一种既实用又经济的最后一英里(Last Mile)或最初一英里(First Mile)的解决方案。

WLL 系统是基于全双工(Full-Duplex)的无线网络，为用户组提供一种类似电话的本地业务。WLL 单元由无线电收发器和 WLL 接口组成，它们统一安装在一个金属盒中。出口处提供两根电缆和一个电话连接器，其中一根电缆连接定向天线(Directional Antenna)和电话插座，另一根连接通用电话装置。如果是传真或计算机通信业务，就连接传真机或调制解调器。WLL 系统中集中了多种无线技术，具体如下所述：

- TDM/TDMA 和 P-MP 通信设备　WLL 系统中使用的通信设备基于时分复用技术和时分多址技术(TDM/TDMA)以及点对多点系统(P-MP)，支持包含基站、中继站和用户站以内的各类业务。
- 固定的蜂窝系统　WLL 系统采用蜂窝电话系统中的无线设备，缩减了对移动功能的使用。用户终端采用蜂窝电话，可以降低系统成本。
- PHS-WLL 系统　WLL 系统采用的是 PHS 终端技术和无线设备。由于语音加密系统采用 32Kb/s 自适应差分脉冲编码调制(ADPCM)方式，所以固定电话的语音质量可以达到标准要求。

(1) WLL 的优势

与有线用户相比，WLL 具有以下优势：

① 网络投资低

随着人力和材料价格的上涨，传统电缆、光缆接入网的费用不断上升。WLL 接入网的投资将比传统电缆、光缆接入网下降 40%左右。

② 建网和扩容快

WLL 不需要铺设缆线，只要把基站和基站控制器等设施安装调试好就可使用，通常只需数周即可完成建网。而有线网至少需要数月甚至数年才能建成。

WLL 扩容更为简单，只要安装用户终端就可迅速提供业务。基站可安装在住户阳台、屋顶等处，无需专用机房。基站安装密度可根据用户多少随意配置，建网时也不必预先知道用户的确切位置。也就是说，可用最少的前期投资为未来市场和业务建立接入网基础设施。

③ 应用范围广

WLL 可解决许多特殊地区电话的普及问题，特别是在人口密度低、线路铺设困难的不平坦地区。在边远地区，由于用户过于分散，设备公用程度很低，网络维护也成问题。采用无线接入设备，可解决这些问题，迅速为用户提供高质量的语音通信。此外，WLL 还可用作城市的第二接入网，为用户业务扩展提供附加线路。

(2) WLL 采用的技术

WLL 系统由基站(BTS)、室内无线终端和用户终端组成。在 WLL 系统中主要采用以下技术：

① 接口信令

接口信令的基本要求是能灵活地支持多种业务的综合接入，它直接关系到 WLL 系统的功能和未来的适应性。现在主要采用的是 V5 接口。对于 V5 接口，主要是指配功能，包括 V5 接口链路配置、C 通路配置、AN 内预连接配置，系统启动前的端口测试控制，V5 接口重新指配和审计信息采集等。V5 接口的物理层是 PCM 链路，可用一般数字中继接口处理。数据链路层和 LAPD 类似，也属于 HDLC 规程的子集，可按照 ISDN PRA 接口或 7 号信令同样的结构处理。根据交换机原有的总体结构，可在数字中继板上一并处理，或将 C 通路提取后接入专用信令板处理。在某些交换机中，ISDN、7 号信令、X.25 和 V5 的第二层均由统一的电路板处理，差别仅在于各类板加载不同的规程处理程序。

② 网络管理系统

网络管理系统是 WLL 的重要组成部分。其功能是对 WLL 各部分进行监视、测试、维护和管理，以保证系统可靠运行。

③ 基站控制软件

基站控制软件是接入网的核心部分。其基本功能是控制 WLL 中的用户呼叫，完成 WLL 和业务网的连接和必要的话务集中。

④ 语音编码技术

新型 WLL 在编码压缩技术方面采用了新的算法，并通过适当增加码速(如采用 13Kb/s)来进一步改善音质，使之与铜线传输的音质相当。不少新的系统直接采用自适应差分脉码调制技术(ADPCM)，并将码速增加到 32Kb/s，其音质与光缆和铜缆传输相当。

⑤ 宽带传输技术

在动态话路指配技术的基础上，当用户需要更宽的频带时，可调节时隙分配，将多个话路合并起来使用，达到宽带传输的作用。

⑥ 动态话路指配技术

为了避免相邻小区间的话路干扰，每话路所使用的载频和时隙可及时动态地调整，从而避免同频干扰，有效地排除各相邻小区间的话路干扰，简化了小区间的频率规划，频率复用不受限制，增加了系统总体容量。

⑦ 无线接口标准选用

目前有三类多址接入方式：频分多址(FDMA)、时分多址(TDMA)和码分多址(CDMA)。FDMA 为模拟系统，采用模拟调频，技术成熟，投资较少，支持语音和低速数据通信，但业务发展潜力不大。后两种方式为数字系统，技术复杂，开发成本较高。其显著优点是通信质量高，保密性好，支持 ISDN 和增值业务，能适应未来通信系统的发展。尤其是 CDMA

系统具有如下所述的独特优点：

- 系统容量大。由于 CDMA 系统是根据伪噪声码实现多址接收的，所有用户可共用一个无线频道，不存在同频复用距离问题。因此其容量远大于 FDMA 和 TDMA 系统。
- 软过载特性。对于给定载频范围，FDMA、TDMA 系统的信道总数恒定，通话用户数达到此值后，就不能再增加了。而当 CDMA 系统话务量达到额定负荷后，通话用户数仍可增加。因此，当话务量很高时，CDMA 系统有瞬时抗过载特性。
- 频率资源共享。无需考虑频率管理和分配，且可与已有 TDMA 及 CDMA 系统共存，共用频率资源。
- 宽带传输，抗多径衰落能力强。由于 WLL 接入的是固定用户，所以在 CDMA 中对系统容量和传输质量影响最大、最难实现的移动台功率自动控制问题，在 WLL 系统中却较易解决，也不存在越区软切换问题。随着技术的日益成熟，CDMA 应是 WLL 系统较理想的可选用无线接口方式。下一部分将对 CDMA 技术进一步展开讨论。

2. CDMA

CDMA 是码分多址(Code-Division Multiple Access)技术的缩写，是近年来在数字移动通信进程中出现的一种先进的无线扩频通信技术，它能够满足市场对移动通信容量和品质的高要求，具有频谱利用率高、语音质量好、保密性强、掉话率低、电磁辐射小、容量大、覆盖广等特点，可以大量减少投资和降低运营成本。

CDMA 被认为是第 3 代移动通信技术的首选，目前的标准有 WCDMA、CDMA2000、TD-SCDMA。

(1) WCDMA

WCDMA 全名是 Wideband CDMA。WCDMA 主要由欧洲 ETSI 和日本 ARIB 提出，其系统的核心网是基于 GSM-MAP 的，同时可通过网络扩展方式提供在基于 ANSI-41 的核心网上运行的能力。

WCDMA 系统支持宽带业务，可有效支持电路交换业务(如 PSTN、ISDN 网)、分组交换业务(如 IP 网)。灵活的无线协议可在一个载波内对同一用户同时支持语音、数据和多媒体业务。通过透明或非透明传输块来支持实时、非实时业务。

WCDMA 采用 DS-CDMA 多址方式，码片速率是 3.84Mb/s，载波带宽为 5MHz。系统不采用 GPS 精确定时，不同基站可选择同步和不同步两种方式，可以不受 GPS 系统的限制。在反向信道上，采用导频符号相干 RAKE 接收的方式，解决了 CDMA 中反向信道容量受限的问题。

WCDMA 采用精确的功率控制，包括基于 SIR 的快速闭环、开环和外环三种方式。功率控制速率为 1500 次/秒，控制步长 0.25dB~4dB 可变，可有效满足抵抗衰落的要求。

WCDMA 还可采用一些先进的技术，如自适应天线(Adaptive antennas)、多用户检测(Multi-user detection)、分集接收(正交分集、时间分集)、分层式小区结构等，来提高整个系统的性能。

WCDMA 技术的优势有：

① 业务灵活性

WCDMA 允许每个 5MHz 载波处理从 8Kb/s~2Mb/s 的混合业务。另外在同一信道上既可以进行电路交换业务也可以进行分组交换业务，利用在单一终端上进行多个电路和分组交换连接，从而实现真正的多媒体业务。可以支持不同质量要求的业务(例如：语音和分组数据)并保证高质量和完美的覆盖。

② 频谱效率

WCDMA 能够高效利用可用的无线电频谱。由于它采用单小区复用，因此不需要频率规划。利用分层小区结构、自适应天线阵列和相干解调(双向)等技术，网络容量可以得到大幅提高。重要的是，由于每个小区层所需要的一切就是 2×5MHz，因此一个分层式网络可在 2×15MHz 频段内部署。

③ 容量和覆盖范围

WCDMA 射频收发信机能够处理的语音用户是典型窄带收发信机的 8 倍。每个射频载波可处理 80 个同时语音呼叫，或者每个载波可处理 50 个同时的 Internet 数据用户。有趣的是，在城市和郊区，WCDMA 的容量差不多是窄带 CDMA 的两倍。

④ 每个连接可提供多种业务

WCDMA 符合真正的 UMTS/IMT-2000 要求。组和电路交换业务可在不同的带宽内自由地混合，并可同时向同一用户提供。每个 WCDMA 终端能够同时接入多达 6 个不同业务，这些业务可以是语音或者传真、电子邮件和视频等数据业务的组合。

⑤ 网络规模的经济性

通过为现有数字蜂窝网络(如欧洲的 GSM)增加 WCDMA 无线接入并运行于两种系统中，同一核心网络可被复用，并使用了相同的站点。WCDMA 接入网络与 GSM 核心网络之间的链路使用了最新的 ATM 模式微型小区传输规程，即异步传输模式第二适配层(AAL2：ATM Adaption Layer 2)。这种高效地处理数据分组的方法将标准 E1/T1 线路的容量提高到了大约 300 个语音呼叫，而现在的网络只有 30 个语音呼叫。预计传输成本将节约 50%左右。

⑥ 无缝的 GSM/UMTS 接入

双模终端将在 GSM 网络和 UMTS/IMT-2000 网络之间提供无缝的切换和漫游，在两个接入系统之间将有尽可能大的业务映象。

⑦ 快速业务接入

为了支持多媒体业务的即时接入，一种新的随机接入机制已经开发出来，它利用快速同步来处理 384Kb/s 分组数据业务。在移动用户和基站之间建立连接所需的时间只有零点几毫秒。

⑧ 低风险成熟技术

在日本和欧洲已经对 WCDMA 评估了多年，爱立信、诺基亚以及日本的 NTTDoCoMo 进行了 WCDMA 的测试工作。在欧洲，自 1989 年起，作为 RACE 项目的一部分，爱立信就开始了 WCDMA 的开发工作。

⑨ 终端的经济性和简单性

WCDMA 手机所要求的信号处理大约是复合 TD/CDMA 技术的十分之一。更简单、更经济的终端易于进行大量生产，从而也就带来了更大的经济规模、更多的竞争，网络运营公司和用户也将获得更大的选择余地。

⑩　从 GSM 升级

WCDMA 使用与 GSM 相同的网络协议结构(信令)，这样将能够使用现有的 GSM 网络作为核心网络基础设施。因此，WCDMA 为 GSM 运营公司提供了在现有投资上建立第三代无线接入的机会。

(2)　CMDA2000

CDMA2000 全名是 Code Division Multiple Access 2000，是从 CDMAOne 蜕变进化出来支援 3G 的一种制式。目的是确保投资发展 CDMA 的网络商，能够简单及有效率地由 CDMAOne 过渡到 3G 进程。共分为两个阶段进化的 CDMA2000，第一阶段将提供 144Kb/s 的数据传送率，而当数据速度加快到 2Mb/s 传送时，便是第二阶段。到时，和 WCDMA 一样，支持移动多媒体服务。

美国 TIA TR45.5 向 ITU 提出的 RTT 方案称为 CDMA2000，其核心是由 Lucent、Motorola、Nortel 和 Qualcomm 联合提出的 Wideband CDMAOne 技术。CDMA2000 的一个主要特点是与现有的 TIA/EIA-95-B 标准向后兼容，并可与 IS-95B 系统的频段共享或重叠，这样就使 CDMA2000 系统可从 IS-95B 系统的基础上平滑地过渡、发展，保护已有的投资。另外，CDMA2000 也能有效地支持现存的 IS-634A 标准。CDMA2000 的核心网是基于 ANSI-41，同时通过网络扩展方式提供在基于 GSM-MAP 的核心网上运行的能力。

CDMA2000 采用 MC-CDMA(多载波 CDMA)方式，可支持语音、分组数据等业务，并且可实现 QoS 的协商。CDMA2000 包括 1X 和 3X 两部分，也可扩展到 6X、9X、12X。对于射频带宽为 N×1.25MHz 的 CDMA2000 系统，采用多个载波来利用整个频带。

CDMA2000 采用的功率控制有开环、闭环和外环三种方式，速率为 800 次/秒或者 50 次/秒。CDMA2000 还可采用辅助导频、正交分集、多载波分集等技术来提高系统的性能。

(3)　TD-SCDMA

TD-SCDMA(时分同步码分多址)，是由大唐电信科技产业集团代表中国提交，并于 2000 年 5 月被国际电联、2001 年 3 月被 3GPP 认可的世界第三代移动通信(3G)的三个主要标准之一。

TD-SCDMA 采用智能天线、软件无线电、联合检测、接力切换、下行包交换高速数据传输等一系列高新技术，与其他系统相比具有以下突出的技术优势：

- 频谱利用率高。与 WCDMA 及 CDMA2000 相比，TD-SCDMA 具有最高的频谱利用率，能够更好支持人口密集地区业务，可以充分利用零碎频段，有效缓解运营商频谱资源紧张的问题。
- 系统容量大。由于采用了诸多先进技术，其干扰大大下降，系统容量大幅提高。
- 特别适合运营商开展数据业务。由于 TD-SCDMA 可以动态调整上下行数据传输速率，特别适合处理上下行不对称的 IP 数据业务。
- 系统成本低。由于采用了智能天线等新技术，TD-SCDMA 系统得以降低发射功率，从而大大降低产品成本。
- 代表移动技术发展方向，系统易于升级，保护运营商投资。目前国际上三代后技术研究的热点包括：TDMA 技术、TDD 技术、智能天线技术、软件无线电技术、下行包交换高速数据传输技术等，这些技术在 TD-SCDMA 系统里已经有所应用。

此外，TD-SCDMA 在通用硬件平台上采用软件无线电技术进行系统设计，升级十分

方便。

TD-SCDMA 标准在国际权威组织中经历了异常严格的检验和测试，完全符合国际上对3G 的全部技术指标要求。它完全满足技术先进性、标准化、公开化的要求，能够作为设备制造商研制和生产 TD-SCDMA 系统设备和运营商使用该设备的技术依据。

10.2.1.2 固定无线接入(FWA)

固定无线接入(FWA)是接入网建设中较重要的解决方案，它具有建设速度快、维护简单、相对成本较低等特点。从技术角度分类，宽带固定无线接入包括 LMDS、MMDS、WDS 和 FSO 等技术。其中应用最为广泛的是工作于高频段(26GHz)的 LMDS 技术和低频段(2.1GHz、2.7GHz、、3.5GHz)的 MMDS 技术。LMDS 频谱资源比较多，可以传输较高的速率，但是由于工作于毫米波，受气候影响大，抗雨衰性能差，降低了在一定地区的可用度；点对多点 MMDS 技术工作在 2.1GHz、2.7GHz、3.5GHz 频段，该频段传输性能好、覆盖范围广(半径 20km)、技术成熟、具有良好的抗雨衰性能、扩容性强、组网灵活且成本具有竞争力，但相对来说传输速率较低。

1. 本地多点分配业务(LMDS)

(1) 概述

本地多点分配业务(Local Multipoint Distribute Service，LMDS)系统是 20 世纪 90 年代后几年出现的热门技术。该系统工作在微波频段的高端 20GHz~40GHz，在较短的传送距离内(3km~10km)实现高容量点到多点微波传输，可提供双向语音、数据及视频图像业务，能够实现从 N×64Kb/s 到 2Mb/s，甚至高达 155Mb/s 的用户接入速率，支持 ATM、TCP/IP、MPEG2 等标准。LMDS 的特征可以从 LMDS 这几个字母体现出来。

- L(本地) 指信号在一个小的覆盖区域内传播。目前在大城市中心进行的现场试验显示 LMDS 发射机的范围最大达 5km。
- M(多点) 指从基站到用户的信号以点到多点或“广播”方式发送，用户到基站的路径是点对点传输方式。
- D(分配) 指信号的分配方式，可同时包括语音、数据、因特网和视频业务，将不同信号分配到不同的接收设备。
- S(业务) 指运营者与用户之间在业务方面是提供与使用的关系，LMDS 网提供的业务完全取决于运营者对网络业务的选择。

目前指的 LMDS 为第 2 代数字系统，主要使用 ATM 传送协议，具有标准化的网络侧接口和网管协议。从理论上讲，LMDS 在上行和下行链路上的传输容量是一样的，因此能方便地提供宽带交互式应用，如电视会议、VOD、住宅用户因特网高速接入等。一个典型的商用 LMDS 系统能提供的下行链路容量为 51.84Mb/s~155.52Mb/s，上行链路则为 1.544Mb/s。在欧洲 LMDS 有时被称为微波视频分配系统(MVDS)，加拿大则称之为本地多点通信系统(LMCS)。

(2) 主要技术要点

目前世界上不少国家都已经规划了 LMDS 的应用频率，主要在 24GHz、26GHz、28GHz、31GHz 和 38GHz 频段，其中，以 27.5GHz~29.5GHz 频段最为集中。欧洲国家主要采用 24GHz~26GHz 及 27GHz~29GHz 频段，而美国 FCC 则选择了 27GHz~31GHz 频段，另外

FCC 还发放了 38GHz 频段的频率。

LMDS 下行主要采用 TDM(时分复用)的方式将信号向相应扇区广播，每个用户终端在特定的时段内接收属于自己的信号。目前绝大多数厂家都采用 ATM 信元流的形式来进行下行业务的分配工作。上行接入时主要采用 TDMA 和 FDMA 两种方式中的一种。

LMDS 的调制方式采用 QPSK(四相相移键控)，也有不少厂家支持 16QAM(正交振幅调制)甚至 64QAM。采用 16QAM，相同频段可以支持的容量是 QPSK 的 2.3 倍，如果采用 QAM，则为 3.5 倍，但是调制技术越复杂，则在相同条件下覆盖的范围越小。

市场上出现的 LMDS 系统基本都采用了无线 ATM 技术，即在无线系统上支持端到端的 ATM 技术。与标准的 ATM 信元相比，无线 ATM 信元还在信元结尾处加入了循环纠错码(CRC)，以便在无线链路上强化纠错功能。在无线 ATM 中，由于信道条件相对恶劣，因此需要极好的差错控制机制，通过前向纠错编码(FEC)和自动反复重发(ARQ)功能有效改善信元丢失率。

由于工作频率处于 20GHz~40GHz 频段，属于受雨衰影响比较严重的 Ka 高频段区内，雨、雪、雾等都会引起传播衰减，造成接收电平降低，较强的降雨甚至可能导致信号的完全中断。为此，LMDS 系统普遍采用了动态自适应发信概率控制技术(ATPC)，一来补偿雨衰，二来减少小区之间的干扰。

LMDS 系统的拓扑结构和局域网类似，可以有星状和环状两种主要的结构形式。目前采用星状结构的比较多。星状结构是指基站采用全向或者扇区天线与用户终端直接进行微波通信。环状结构是指相邻基站之间采用定向天线彼此进行微波通信，中央节点位于网络枢纽位置，负责微波环路上业务量的汇聚和转接。环状 LMDS 可以方便地实现链路自愈能力。相对来说，星状拓扑结构比较适合用户分布比较确定和较为集中的环境，环状结构则比较适合用户比较稀少、地理环境比较复杂的情况。

(3) LMDS 系统结构

LMDS 系统是一个从用户终端到核心网络的接入平台，组网方案相当灵活，基本采用蜂窝式的结构配置。一个完整的 LMDS 系统由核心(骨干)网络、基站系统、用户驻地设备和网管系统构成。

骨干网络即指 PSTN、ISDN、ATM、帧中继、因特网等网络。基站系统通过多扇区覆盖的方式向所需要地区提供连接，主要提供 LMDS 系统至核心网络的接口，完成信号在核心网络至无线传输之间的转换并负责无线资源的管理。基站系统包括与核心网络连接的接口模块、调制与解调模块及射频收发模块组成。

用户驻地设备也称终端设备，主要负责将用户连接到基站。用户驻地设备的配置差异较大，不同的设备供应商有不同的技术选择，一般说来都包括室外单元(含定向天线、微波收发设备)与室内单元(含调制与解调模块以及与用户室内设备相连的网络接口模块)。用户室外单元通常采用口径很小(30cm)的室外定向天线就可以满足要求，安装很方便。

LMDS 网管系统多数是基于 TCP/IP 协议的简单网络管理协议(SNMP)，主要负责管理多个区域内的用户网络，负责完成告警与故障诊断、系统配置、计费、系统性能分析和安全管理等功能。

2. 多点多信道分配系统(MMDS)

MMDS 系统即多点多信道分配系统，最初由美国提出，在 2.5GHz~2.7GHz 频段上使

用，单向传送视频信号。目前典型的 MMDS 系统结构由中心站(基站)设备(卫星信号接收设备、无线收发信机、其他的广播设备和传输天线)以及用户驻地的接收设备(天线、频率转换设备、机顶盒)组成。小区覆盖范围大约在 35 英里，主要取决于广播功率，基站广播功率一般在 1W~100W。

MMDS 是一种点对多点分布、提供宽带业务的无线技术。它适用于中小企业用户和集团用户。MMDS 可透明传输业务，在基站端与网络的接口为 T1/E1、100Base-T 和 OC-3 等，在用户端的接口为 E1 和 10Base-T 等，可以为用户提供 Internet 的接入、本地用户的数据交换、语音业务和 VOD 视频点播业务。MMDS 主要集中在 2GHz~5GHz 频段。相对而言，这个频段的资源比较紧张，各国能够分配给 MMDS 使用的频率要比 LMDS 少得多。由于 2GHz~5GHz 频段受雨衰的影响很小，并且在同等条件下空间传输损耗也较 LMDS 低，所以 MMDS 频段可应用于半径为几十公里的大范围覆盖。

MMDS 最初用于传输单向电视和网络广播，1970 年 FCC 在 2.5GHz 上划分了 200MHz 给无线电信运营商，其中共有 31 个信道，每信道带宽为 6MHz。虽然 MMDS 的技术不断革新，但是当时的市场情况并不成熟，也没有受到足够的重视。近来，高速数据接入的发展促进了 MMDS 的发展，1998 年 9 月，FCC 批准运营商采用双向的数据业务传输，允许更加灵活地使用 MMDS 频段。同时 MMDS 的数字化发展也使得它更具竞争力。

MMDS 适用于用户分布很分散的情况。但是，由于信道数量的限制，对运营商而言，用更高调制技术的方式来提高应用频率是很冒险的，这是限制 MMDS 在大型商业区应用的最重要的一点，而且大的覆盖范围也容易引起 MMDS 小区之间的干扰。

与点对多点的 LMDS 相比，MMDS 适于用户相对分散、容量较小的地区，从成本上来讲，MMDS 低于 LMDS。MMDS 所能提供的数据带宽同样与可利用的频段、采用的调制方式(QPSK、16QAM 或 64QAM)和扇区数量有关。粗略估算，能够提供的容量大约为所占频率带宽的 3~4 倍，即 100MHz 的频率带宽能提供 300Mb/s~400Mb/s 的数据带宽，供一个基站覆盖范围内的用户共享。MMDS 同样能够作为 IP、TDM 和帧中继等接入骨干网络的宽带无线接入解决方案。用户通过它可以实现 Internet 接入、本地用户大容量数据交换、语音、VoIP、VOD、数据广播和标准清晰度或高清晰度电视信号等多种业务。

10.2.1.3 无线局域网(WLAN)

WLAN 利用无线技术在空中传输数据、语音和视频信号。作为传统布线网络的一种替代方案或延伸，无线局域网把个人从办公桌边解放了出来，使他们可以随时随地获取信息，提高了员工的办公效率。此外，WLAN 还有其他一些优点。它能够方便地实施联网技术，因为 WLAN 可以便捷、迅速地接纳新加入的雇员，而不必对网络的用户管理配置进行过多的变动。WLAN 还可以在有线网络布线困难的地方比较容易实施，使用 WLAN 方案，则不必再实施打孔敷线作业，因而不会对建筑设施造成任何损害。

目前，无线局域网有许多标准。例如，IEEE 802.11、IEEE 802.11b、IEEE 802.11a、IEEE 802.11g、蓝牙、HomeRF 等。目前国内国际上采用的无线局域网技术主要是由思科、3Com、Promix、英特尔和杰尔公司共同创立的 802.11b 标准，传输率为 11Mb/s。

1.802.11 家族

(1) IEEE 802.11

1997 年 6 月，IEEE 推出了第 1 代 WLAN 标准——IEEE 802.11(1997 版)，随后在 1999 年推出了新的 IEEE 802.11(1999 版)。该标准定义了物理层和媒介访问控制子层(MAC)的技术规范，允许 WLAN 及无线设备制造商在一定范围内建立互操作网络设备。任何 LAN 应用、网络操作系统或协议(包括 TCP/IP 和 Novell NetWare)在遵守 IEEE 802.11 标准的无线 LAN 上运行时，都像它们运行在以太网上一样容易。

IEEE 802.11 在物理层定义了数据传输的信号特征和调制方法，定义了两种无线电射频(RF)传输方式和一种红外线传输方式。其中 RF 传输标准包括直接序列扩频技术(Direct Sequence Spread Spectrum，DSSS)和跳频扩频技术(Flequency Hopping Spread Spectrum，FHSS)。DSSS 采用一个长度为 11 比特的 Barker 序列来对以无线方式发送的数据进行编码。每个 Barker 序列表示一个二进制数据位(1 或 0)，并被转换成可以通过无线方式发送的波形信号。这些波形信号如果使用二进制相移键控(BPSK)调制技术，可以以 1Mb/s 的速率进行发射；如果使用正交相移键控(QPSK)调制技术，发射速率可以达到 2Mb/s。FHSS 利用 GFSK 二进制或四进制调制方式可以达到 2Mb/s 的工作速率。

由于在无线网络中碰撞检测较困难，IEEE 802.11 规定媒介访问控制(MAC)子层采用碰撞回避(CA)协议，而不是碰撞检测(CD)协议。为了尽量减少数据的传输碰撞和重试发送，防止各站点无序争用信道，WLAN 中采用了与以太网 CSMA/CD 相类似的 CSMA/CA(载波侦听多址访问/碰撞回避)协议。CSMA/CA 通信方式将时间域的划分与帧格式紧密联系起来，保证某一时刻只有一个站点发送，实现了网络系统的集中控制。因传输媒介不同，CSMA/CD 与 CSMA/CA 的检测方式也不同。CSMA/CD 通过电缆中电压的变化来检测，当数据发生碰撞时，电缆中的电压就会随着发生变化；而 CSMA/CA 采用能量检测(ED)、载波检测(CS)和能量载波混合检测三种检测信道空闲的方式。

(2) IEEE 802.11b

由于现行的以太网技术可以实现 10Mb/s，100Mb/s 乃至 1000Mb/s 等不同速率以太网络之间的兼容，为了支持更高的数据传输速率，IEEE 于 1999 年 9 月批准了 IEEE 802.11b 标准。IEEE 802.11b 标准对 IEEE 802.11 标准进行了修改和补充，其中最重要的改进就是在 IEEE 802.11 的基础上增加了 5.5Mb/s 和 11Mb/s 两种更高的通信速率。因此有了 IEEE 802.11b 标准之后，移动用户将可以得到以太网级的网络性能、速率和可用性，管理者也可以无缝地将多种 LAN 技术集成起来，形成一种能够最大限度地满足用户需求的网络。IEEE 802.11b 的基本结构、特性和服务仍然由最初的 IEEE 802.11 标准定义。IEEE 802.11b 技术规范只影响 IEEE 802.11 标准的物理层，提供了更高的数据传输速率和更牢固的连接性。

为了使 IEEE 802.11b 支持 5.5Mb/s 和 11Mb/s 两种速率。需要选择 DSSS 作为该标准的惟一物理层技术，因为，目前在不违反 FCC 规定的前提下，采用跳频扩频技术无法支持更高的速率。这意味着 IEEE 802.11b 系统可以与速率为 1Mb/s 和 2Mb/s 的 IEEE 802.11 DSSS 系统兼容，但却无法与速率为 1Mb/s 和 2Mb/s 的 IEEE 802.11 FHSS 系统兼容。

为了增加数据通信速率，IEEE 802.11b 标准没有使用 11 比特长的 Barker 序列，而是采用了补充编码键控(CCK)，CCK 由 64 个 8 比特长的码字组成。作为一个整体，这些码字具有自己独特的数据特性，即使在出现严重噪声和多方干扰的情况下，接收方也能够正确地

予以区别。IEEE 802.11b 规定在速率为 5.5Mb/s 时使用 CCK，对每个载波进行 4 比特编码；而当速率为 11Mb/s 时，对每个载波进行 8 比特编码。这两种速率都使用 QPSK 作为调制技术。

(3) IEEE 802.11a

IEEE 802.11a 标准是已在办公室、家庭、宾馆和机场等众多场合得到广泛应用的 IEEE 802.11b 无线组网标准的后续标准。IEEE 802.11a 工作在 5GHz U-NII 频带，物理层速率可达 54Mb/s，传输层可达 25Mb/s。IEEE 802.11a 选择具有能有效降低多径衰落影响与有效使用频率的正交频分复接(OFDM)为调制技术，可提供 25Mb/s 的无线 ATM 接口和 10Mb/s 的以太网无线帧结构接口，以及 TDD/TDMA 的空中接口；支持语音、数据和图像业务；一个扇区可接入多个用户，每个用户可带多个用户终端。

(4) IEEE 802.11g

由于下一代规格 IEEE 802.11a 与目前的 IEEE 802.11b 规范之间频段与调制方式的不同，使得两者不能互通，已经拥有 IEEE 802.11b 产品的消费者可能不会在 IEEE 802.11a 设备问世之后就立即购买；而 IEEE 802.11g 就是为这段过渡时间所发展的规范，它构建在既有的 IEEE 802.11b 物理层与介质层标准基础上，选择 2.4GHz 频段、传输速率较 11Mb/s 高，让已拥有 IEEEE802.11b 产品的使用者能够以 IEEE 802.11g 的产品满足速度升级的需求。

在 2000 年初，IEEE 802.11g 的工作组接受了一项开发高速、向下兼容非常成功的 IEEE 802.11b 物理层标准的工作，新增的 IEEE 802.11g 标准将兼容 IEEE 802.11b 的 MAC，实现所有 IEEE 802.11b 所必要的功能并保证兼容、可交互，同时包括至少 20Mb/s 的速度，还包括 2.4GHz/5GHz 波段的融合，从而在 2.4GHz 频段获得更高的速度。

IEEE 802.11g 工作组几乎用了一年半的时间，在集中的建议中取得了一个折中的方案，这成为了 2001 年 11 月的第一个 IEEE 802.11g 草案。工作组在 2002 年 1 月份的会议上还取得了一些附加的技术改善效果。

IEEE 802.11g 草案采用了 IEEE 802.11b 标准的要求，在 2.4GHz 频段速度可扩展至 54Mb/s。在 IEEE 802.11g 里，IEEE 802.11b 的标准模式是必须具备的，如 1/2Mb/s 巴克码、5.5/11Mb/s 补充编码键控(CCK)、和 192μs 的长前导同步码。除此之外，IEEE 802.11g 规定 96μs 短前导同步码是 IEEE 802.11b 的选项，从而增加吞吐量。IEEE 802.llg 的最重要的方面是向后兼容 IEEE 802.11b，特别是短数据包。IEEE 802.11b 中的可选的 5.5/11Mb/s 数据包二进制卷积码在 IEEE 802.11g 中被扩展到 22Mb/s 和 33Mb/s。

为取得 54Mb/s 的速率，IEEE 802.11g 草案借用了 IEEE 802.11a。IEEE 802.11a 在 5GHz 频段采用了正交频分复用(OFDM)，可以取得 6Mb/s，9Mb/s，12Mb/s，18Mb/s，24Mb/s，36Mb/s，48Mb/s 和 54Mb/s 的速率。IEEE 802.11g 在 2.4GHz 频段采用了同样的编码格式取得了同样的速率，规定 OFDM 速率为 6Mb/s，12Mb/s 和 24Mb/s。为补偿 IEEE 802.11 标准 16μs 的帧间隙和 IEEE 802.11g 标准 10μs 的帧间隙，在 OFDM 数据包中增加了 6μs 的虚拟的信号扩展：在这 6μs 期间，没有信号传输，但 MAC 层伪装成有数据传输。结果是一个更长的 16μs 的帧间隙，这对 OFDM 数据包解码是需要的。

IEEE 802.11g 草案附加的可选模式是 CCK-OFDM，它使用巴克码做前导同步码和 OFDM 数据编码。CCK-OFDM 方案也支持 6Mb/s，9Mb/s，12Mb/s，18Mb/s，24Mb/s，36Mb/s，48Mb/s 和 54Mb/s 的数据编码。

在 5GHz 频段 WLAN 标准的协调方案有更多的工作，比如 IEEE 802.11a 和 HiperLAN2，IEEE 802.11g 都会影响 2.4GHz 和 5GHz 频段的协调，因为 IEEE 802.11a 和 IEEE 802.11g 的 OFDM 编码方案是一致的，IEEE 802.11g 比起 IEEE 802.11a 有更多的功能，这个事实引起了 IEEE 802.11a 和 IEEE 802.11g 混合产品的广泛讨论。注意 IEEE 802.11g 实际上是 IEEE 802.11a 的补充，这种混合产品称做 IEEE 802.11abg。事实上，这在 IEEE 802.11g 的第一个草案里称做 a+b=g。

通过使用相同的频段，IEEE 802.11g 允许制造商继续支持和扩展所有 2.4GHz 频段高性能、高集成产品的开发。由于 2.4GHz 频段在国际上的广泛使用，这也使得并发出的产品在许多国家可以使用。

2. 蓝牙

(1) 什么是蓝牙

所谓蓝牙(Bluetooth)技术，实际上是一种短距离无线电技术，利用“蓝牙”技术，能够有效地简化掌上电脑、笔记本电脑和移动电话手机等移动通信终端设备之间的通信，也能够成功地简化以上这些设备与 Internet 之间的通信，从而使这些现代通信设备与 Internet 之间的数据传输变得更加迅速高效，为无线通信拓宽道路。说得通俗一点，就是蓝牙技术使得现代一些轻易携带的移动通信设备和电脑设备实现无线上 Internet，其实际应用范围还可以拓展到各种家电产品、消费电子产品和汽车等信息家电，组成一个巨大的无线通信网络。“蓝牙”技术属于一种短距离、低成本的无线连接技术，是一种能够实现语音和数据无线传输的开放性方案。因此，目前虽然无线通信的“蓝牙”刚刚露出一点儿芽尖，却已经引起了全球通信业界和广大用户的密切关注。

(2) 蓝牙的由来

蓝牙以公元 10 世纪统一丹麦和瑞典的一位斯堪的纳维亚国王的名字命名。它孕育着颇为神奇的前景：对手机而言，与耳机之间不再需要连线；在个人计算机，主机与键盘、显示器和打印机之间可以摆脱纷乱的连线；在更大范围内，电冰箱、微波炉和其他家用电器可以与计算机网络的连接，实现智能化操作。

发明蓝牙技术的是瑞典电信巨人爱立信公司。由于这种技术具有十分可喜的应用前景，1998 年 5 月，五家世界顶级通信/计算机公司：爱立信、诺基亚、东芝、IBM 和英特尔公司经过磋商，联合成立了蓝牙共同利益集团(Bluetooth SIG)，目的是加速其开发、推广和应用。此项无线通信技术公布后，便迅速得到了包括摩托罗拉、3Com、朗讯、康柏、西门子等一大批公司的一致拥护，至今加盟蓝牙 SIG 的公司已达到 2000 多个，其中包括许多世界最著名的计算机、通信以及消费电子产品领域的企业，甚至还有汽车与照相机的制造商和生产厂家。一项公开的技术规范能够得到工业界如此广泛的关注和支持，这说明基于此项技术的产品将具有广阔的应用前景和巨大的潜在市场。蓝牙共同利益集团现已改称蓝牙推广集团。

(3) 蓝牙的技术内容

蓝牙技术产品采用低能耗无线电通信技术来实现语音、数据和视频传输，其传输速率最高为 1Mb/s，以时分方式进行全双工通信，通信距离为 10m 左右，配置功率放大器可以使通信距离进一步增加。

蓝牙产品采用跳频技术，能够抗信号衰落；采用快跳频和短分组技术，能够有效地减

少同频干扰，提高通信的安全性；采用前向纠错编码技术，以便在远距离通信时减少随机噪声的干扰；采用 2.4GHz 频段，以省去申请专用许可证的麻烦；采用 FM 调制方式，使设备变得更为简单可靠；“蓝牙”技术产品一个跳频频率发送一个同步分组，每一个分组占用一个时隙，也可以增至 5 个时隙；“蓝牙”技术支持一个异步数据通道，或者 3 个并发的同步语音通道，或者一个同时传送异步数据和同步语音的通道。“蓝牙”的每一个语音通道支持 64Kb/s 的同步语音，异步通道支持的最大速率为 721Kb/s、反向应答速率为 57.6Kb/s 的非对称连接，或者 432.6Kb/s 的对称连接。

10.2.1.4 卫星接入

因特网上网用户数量在急剧增加，其应用范畴正在向交互式多媒体方向快速发展，为此，需要宽带传输系统予以支撑。当前，开发大容量宽带光纤网络平台并解决好最后一英里的问题，已成为 IT 业界研发的热点。与此同时，鉴于卫星通信具有广播特性，以及卫星链路具有建设快且费用低的优点，利用宽带卫星链路接入 Internet(IP over satellite)的业务也在迅速发展中。目前，已在运营的一些 GEO 卫星通信系统可以提供高达 45Mb/s 的下行数据流(downstream)，有的系统还可提供 30Mb/s 双向(上行和下行)数据流。一些正在发展中的天空因特网(Internet in the sky)将有可能提供速率更高的双向数据流。

在目前还没有良好的地面通信基础设施的地方，诸如边远地区、山村和海岛等，卫星通信链路可以充当接入 Internet 的主角。在这些地区建立卫星链路，既便宜又方便。在某些发达国家或地区，即使其地面基础设施已十分充足，且带宽足够使用，利用卫星链路作为地面系统的补充或应急备用，仍然是必要的。

许多 Internet 用户受限于当地 ISP 提供的语音等级拨号接入，带宽只有 56Kb/s，要想得到更高的数据速率，费用相当可观。利用价廉的卫星 VSAT 装在屋顶，对提高数据速率十分方便。

卫星可为 ISP 提供直接的数据传输基础结构，传输可以是双向对称的或不对称的。可方便地改变传输速率，一般可以从 128Kb/s 或 256Kb/s 开始，必要时可加倍、再加倍。

利用卫星链路接入，可以旁路因特网瓶颈，避免拥塞。用户在链路上进行点击，向远方服务器查寻资料，其信息量是以 Byte 计算的；反之，当所查寻的图形、网页、文件或音频/视频信息流由远端发送给查寻者及其浏览器时，其信息量将以千字节甚至兆字节计。大信息流的增长很容易使网络拥塞，形成瓶颈。网络层次和连接次数的增加也是产生瓶颈的重要因素。据统计，每个万维网超链(Web hyperlink)点击加上随后的网页、文件等下载，所通过的路径总数平均多达 18 个。路由层次多不仅容易使网络拥塞，且每次连接都须付出成本和处理时间。利用 GEO 卫星链路可以最大限度地旁路地面基础结构中易于拥塞的路由，并能尽可能地减少通过的网络层次。

在现代 Internet 应用中，往往是一个内容要求同时发往几个或多个接收者，这种应用一般称为多址播发或多播(multicasting)。多播业务大约占 Internet 总业务量的 30%。地面系统多播的老办法是一个一个地重复发送，直到发完为止。这种处理方法，效率自然很低，发送短消息尚可接受，如果发送大文件，将大大浪费信道带宽和各种相关设备的处理时间。较新的多播技术是将多播信息通过路由器构成的传递树来传输。这种传输协议较晚时才加进 IPv4 中，目前一些路由器还不能支持。还有一种称为隧道(tunneling)的技术能把特定的

局部地区联接起来进行多播。但是，在地面网络中能同时参加多播的接收者数量仍然受到一定限制。相比之下，利用 GEO 卫星进行多播则效果很好。在卫星覆盖范围内，任何地址都可以接收卫星数据。建立起卫星星际链路(ISL)系统可能将同一信息数据发往全球。现代接收卫星下行线的小型天线和接收机都相当便宜，一个 WAN 可以很快地利用卫星系统扩大，而所需费用仅为利用地面线路时投资的很小部分。

10.2.2　典型例题分析

例 1　目前，通过移动电话接入互联网所采用的主要技术是什么？(2004 年上半年下午试题一)

分析：通过移动和无线通信系统接入因特网的方式分为两大类，一是基于蜂窝数字电话的接入技术，如 CDPD，GPRS，EDGE 和 2.5G CDMA 技术等；二是基于局域网的技术，如 IEEE 802.11 WLAN，Bluetooth，HomeRF 等。

目前，包括 GPRS 和 2.5G CDMA 在内的 2G+移动技术解决了手机接入互联网的问题。GPRS 的全名为 General Packet Radio Service，即通用分组无线服务，它是利用“分组交换”的概念发展出的一套无线传输方式。采用分组交换的是一种比电路交换更加适合传输数据的方式，频带利用率更高。GPRS 可以提供四种不同的编码方式，这些编码方式也分别提供不同的错误保护能力。利用四种不同的编码方式，每个时槽可提供的传输速率为 CS-l(9.05Kb/s)、CS-2(13.4Kb/s)、CS-3(15.6Kb/s)及 CS-4(21.4Kb/s)。每个用户最多可同时使用 8 个时槽，所以 GPRS 的最高传输速率为 171.2Kb/s，比传统的拨号速度要快，基本能满足简单数据业务的需求。

2.5G CDMA 是 CDMA 技术标准系列中的一环。它的基础是属于移动通信 2G 标准的 TIA/EIAIS-95，是和 GSM 并列的移动通信技术。CDMA 也有 2 代、2.5 代和 3 代技术，目前国内使用的 CDMA 系统是 2.5G 的 CDMA1x 技术标准。它拥有频率利用率较高、手机功耗低等优点，能满足无线用户高速数据交换的要求，而且它可以直接升级到真正的 3G 网络 CDMA2000。

与此同时，还有很多的无线接入技术标准，它们都是侧重不同的层次，比如 Bluetooth 是针对网络接口层的移动性而提出的，而 Mobile IP 则针对网络层。这些技术也可以组合运用，WAP(Wireless Application Protocol)实现了基于 WAP 浏览器的手机能获取一系列新的增值服务，是一个开放的全球标准，可以使移动电话和其他无线终端的用户快速安全地获取互联网及企业内部网的信息及其他通信服务。WAP 融合了网络接口层解决方案的现有成果，引入了针对传输层的 WDP(无线数据报协议)，解决了标准 HTML 内容无法在手机及呼机的小屏幕上有效显示问题，所以可以把 WAP 归结为应用层的解决方案。

答案：GPRS 和 CDMA。

例 2　目前，国内采用的第三代移动通信技术标准有哪些？(2004 年上半年下午试题一)

分析：按 ITU 总目标，第三代移动通信系统有如下特点：提供高速率和多种速率；支持多种业务；能支持从语音到分组数据、多媒体业务，特别是因特网；应能根据需要来提供必要的带宽。其最低无线传输要求如下：

(1) 快速移动环境　最高速率达 114Kb/s。

(2) 步行环境 最高速率达384Kb/s。

(3) 室内环境 最高速率达2Mb/s。

ITU针对3G规定了5种陆地无线技术，其中WCDMA、CDMA2000和TD-SCDMA是3种主流技术。在这3种技术中，WCDMA和CDMA2000采用频分双工(FDD)方式，需要成对的频率规划。WCDMA即宽带CDMA技术，其扩频码速率为3.84Mchip/s，载波带宽为5MHz；CDMA2000的扩频码速率为1.2288Mchip/s，载波带宽为1.25MHz。另外，WCDMA的基站间同步是可选的，CDMA2000的基站间同步是必需的，因此需要全球定位系统(GPS)，以上是WCDMA和CDMA2000最主要的区别。TD-SCDMA采用时分双工(TDD)、TDMA/CDMA多址方式工作，扩频码速率为1.28Mchip/s，载波带宽为1.6MHz，其基站间必须同步，与其他两种技术相比，TD-SCDMA采用了智能天线、联合检测、上行同步及动态信道分配、接力切换等技术，具有频谱使用灵活、频谱利用率高等特点，适合非对称数据业务。

目前，因为信息产业部还没有发放3G牌照，国内两大移动运营商中国移动和中国联通都还没有真正意义上的3G网络，但是中国联通的CDMA网络从最早的2G的CDMA95升级为2.5G的CDMA1x，具备了较高速度的数据传输速度，但不是真正意义上的3G，而CDMA1x是CDMA技术标准系列中的一环。它的基础是属于移动通信2G标准的TIA/EIAIS-95。其下一步则是属于移动通信3G标准CDMA2000。CDMAlx手机上网的传输速率可达144Kb/s，比此前属于2G标准的CDMA95高出10倍。国内的厂商大唐电信所提议的3G标准TD-SCDMA也还没有进入商用的阶段。目前全球已经颁发了73个WCDMA运营牌照，13个CDMA2000运营牌照。中国移动和中国联通等运营商将采用何种技术标准目前仍未确定。不久前，信息产业部已经对WCDMA、CDMA2000、TD-SCDMA的使用频率进行了规划，预示着这三种标准在中国都将被采用。

答案：WCDMA、CDMA2000和TD-SCDMA。

例3 列举IEEE 802.11b的两种运作模式。

分析：IEEE 802.11b的运作模式分为两种：点对点模式和基本模式。点对点模式是指无线网卡和无线网卡之间的通信方式。基本模式是IEEE 802.11b最常用的方式，是无线网络通过接入点(Access Point)与有线网络相连的通信方式，在这种模式下，接入点AP充当了无线网和有线网之间的桥梁。这样，无线局域网既可作为对有线网络的补充，也可独立组网，从而使网络用户摆脱网线的束缚，实现真正意义上的移动应用。

答案：点对点模式和基本模式。

例4 从工作的频段、数据传输速率、优缺点以及它们之间的兼容性等方面，对IEEE 802.11a、IEEE 802.11b和IEEE 802.11g进行比较。(2004年下半年下午试题一)

分析：IEEE 802.11a在5GHz频段采用了正交频分复用(OFDM)，可以取得6Mb/s，9 Mb/s，12 Mb/s，18 Mb/s，24 Mb/s，36 Mb/s，48 Mb/s和54Mb/s的速率。

IEEE 802.11b规定采用2.4GHz频带，调制方法采用补偿码键控(CCK)，共有3个不重叠的传信道。传输速率能够从11Mb/s自动降到5.5Mb/s。在速率为5.5Mb/s时使用CCK，对每个载波进行4比特编码；而当速率为11Mb/s时，对每个载波进行8比特编码。这两种

速率都使用 QPSK 作为调制技术。

IEEE 802.11g 草案采用了 IEEE 802.11b 标准的要求，在 2.4GHz 频段速度可扩展至 54Mb/s。在 IEEE 802.11g 里，IEEE 802.11b 的标准模式是必须具备的，如 1/2Mb/s 巴克码、5.5/11Mb/s 补充编码键控(CCK)和 192μs 的长前导同步码。除此之外，IEEE 802.11g 规定 96μs 短前导同步码是 IEEE 802.11b 的选项，从而增加吞吐量。IEEE 802.llg 的最重要的方面是向后兼容 IEEE 802.11b，特别是短数据包。IEEE 802.11b 中的可选的 5.5/11Mb/s 数据包二进制卷积码在 IEEE 802.11g 中被扩展到 22Mb/s 和 33Mb/s。IEEE 802.11g 草案附加的可选模式是 CCK-OFDM，它使用巴克码做前导同步码和 OFDM 数据编码。CCK-OFDM 方案也支持 6 Mb/s，9 Mb/s，12 Mb/s，18 Mb/s，24 Mb/s，36 Mb/s，48 Mb/s 和 54Mb/s 的数据编码。

若想进一步了解可以参考 10.2.1.3 节内容。

答案：略。

10.2.3　同步练习

1. 固定无线接入(FWA)有哪两种方式？对这两种方式进行比较。
2. 提高 WLAN 的安全性有哪些措施？
3. 简述 802.1x 的认证过程。
4. 列举蓝牙产品采用的主要技术内容。

10.2.4　同步练习参考答案

1. 本地多点分配业务(LMDS，Local Multipoint Distribute Service)系统工作在微波频段的高端 20GHz~40GHz，在较短的传送距离内(3km~10km)实现高容量点到多点微波传输，可提供双向语音、数据及视频图像业务，能够实现从 N×64Kb/s 到 2Mb/s，甚至高达 155Mb/s 的用户接入速率，支持 ATM、TCP/IP、MPEG2 等标准。

MMDS 系统即多点多信道分配系统。MMDS 主要集中在 2GHz~5GHz 频段。由于 2GHz~5GHz 频段受雨衰的影响很小，并且在同等条件下空间传输损耗也较 LMDS 低，所以 MMDS 频段可应用于半径为几十公里的大覆盖范围。

与点对多点的 LMDS 相比，MMDS 适于用户相对分散、容量较小的地区，从成本上来讲，MMDS 低于 LMDS。MMDS 同样能够作为 IP、TDM 和帧中继等接入骨干网络的宽带无线接入解决方案。用户通过它可以实现 Internet 接入、本地用户大容量数据交换、语音、VoIP、VOD、数据广播和标准清晰度或高清晰度电视信号等多种业务。

2. (1)扩频、跳频无线传输技术本身使盗听者难以捕捉到有用的数据；(2)设置严密的用户口令及认证措施，防止非法用户入侵；(3)设置附加的第三方数据加密方案，即使信号被盗听也难以理解其中的内容；(4)采取网络隔离及网络认证措施。

3. 802.1x 的认证过程如下：

(1) 最初的 802.1x 通信开始以一个非认证客户端设备尝试去连接一个认证端(如 AP)，客户端发送一个 EAP 起始消息。然后开始客户端认证的一连串消息交换。

(2) AP 回复 EAP 请求身份消息。

(3) 客户端发送给认证服务器的 EAP 的响应信息包里包含了身份信息。AP 通过激活

一个只允许从客户端到 AP 有线端的认证服务器的 EAP 包的端口，并关闭了其他所有的传输，像 HTTP、DHCP 和 POP3 包，直到 AP 通过认证服务器来验证用户端的身份(例如：RADIUS)。

(4) 认证服务器使用一种特殊的认证算法去验证客户端身份。同样它也可以通过使用数字认证或其他类型的 EAP 认证。

(5) 认证服务器会发送同意或拒绝信息给这个 AP。

(6) AP 发送一个 EAP 成功信息包(或拒绝信息包)给客户端。

(7) 如果认证服务器认可这个客户端，那么 AP 将转换这个客户端的端口到授权状态并转发其他的通信。最重要的是，这个 AP 的软件是支持认证服务器里特定的 EAP 类型的，并且用户端设备的操作系统里或客户端应用软件也要支持它。AP 为 802.1x 消息提供了“透明传输”。这就意味着你可以指定任一 EAP 类型，而不需要去升级一个自适应 802.1x 的 AP。

4. 蓝牙产品采用跳频技术来抗信号衰落；采用快跳频和短分组技术来有效地减少同频干扰，提高通信的安全性；采用前向纠错编码技术来在远距离通信时减少随机噪声的干扰。

10.3 主 干 网

10.3.1 考点辅导

10.3.1.1 IP over SDH/SONET

IP over SDH/SONET 有两个国际标准，一个是 ITU-T 的 X.85(用 LAPS 的 IP over SDH)，另一个是 IETF 的 RFC 2615(PPP over SDH/SONET)。

SDH 为同步数字体系，其复用方法、规定的 SDH 比特率、一般原理以及帧结构等内容由 G.707 建议，即同步数字体系(SDH)的网络节点接口规定。

SDH 的信号由一个或多个不同阶的同步传送模块(STM-N)信号组成。基本模块 STM-1 信号的速率是 155.520Mb/s，而 STM-N 信号的速率是 N×155.520Mb/s。STM-N 信号的帧结构如图 10.1 所示，它由三个区域组成，分别为段开销(SOH)、管理单位指针(AUPTR)、净负荷(Payload)。

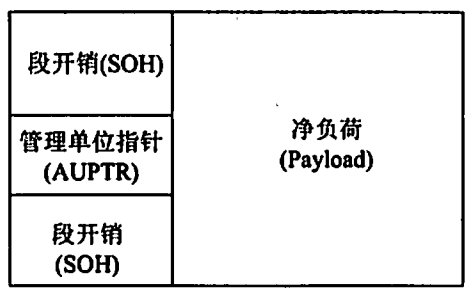


图 10.1 STM-N 帧结构

SIM-N 帧可表示成二维的块状帧结构。纵向有 270×N 列，横向有 9 行，共计为 2430×N 字节。帧重复周期为 125μs。传输时逐字节从左到右、从上到下逐行进行，为串行传输。对于 STM-1，净负荷是从第 10 列起到第 270 列共 261 列(2349 个字节)，可用于传送 LAPS 帧(或 PPP 帧)，而 LAPS 帧(或 PPP 帧)的信息字段包含了一个或多个 IP 包。

SDH 设备包括 SDH 线路系统、DXC/ADM、光电接口、管理模块等。DXC 是数字交叉连接设备，ADM 是分插复用器。线路系统是最基本部分，DXC/ADM 可提供更广泛的 VC 连接，实现完全的 SDH 网。一般环形节点用 ADM 构成，利用 ADM 的分插能力和智能构成自愈环，即当局部线路或设备出现故障时，可用备份替换故障部分。SDH 的线路速率可根据业务量的需要选用 STM-1(155.520Mb/s)或 STM-N(N×155.520Mb/s)。

SONET 是美国 ANSI 为光媒体上同步数据传输制定的标准，是 SDH 的前身，即 SDH 是在 SONET 的基础上发展起来的。通常 SONET 系统广泛用于北美。其基本结构与 SDH 相同，但具体细节不相同。

用 LAPS 的 IP over SDH(X.85 建议)协议栈的结构如图 10.2 所示。

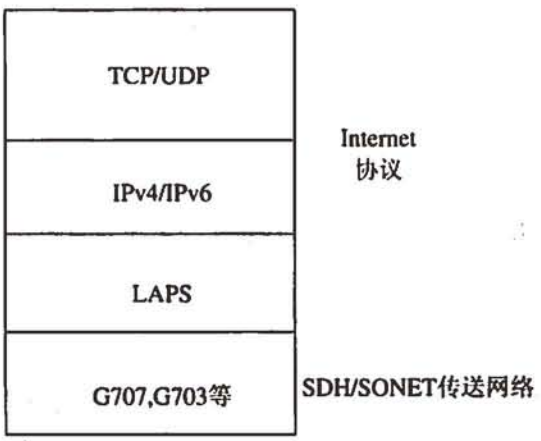


图 10.2　IP over SDH 协议栈的结构

传送层协议为 TCP 及 UDP，网络层协议为 IPv4、ICMP，IPv6、ICMPv6，链路层协议为 LAPS，物理层协议为 G.707、G.703 等。X.85 也可支持 PPP 协议。

用 LAPS 的 IP over SDH 的标准为 ITU-T X.85 建议。上述协议结构是 X.85 协议所规定的。实际上在 X.85 协议未规定前，用 PPP over SDH/SONET IP 包通过 PPP 包在 SDH/SONET 网中传输，所以早先的 IP over SDH/SONET 也称 Pocket over SDH/SONET，简称 POS。X.85 设计时已考虑了与 PPP over SDH/SONET 的兼容。

X.85 协议规定的线路速率：

依据 G.707 为 STM-1、STM-4、STM-16、STM-64，分别为：155.52 Mb/s、155.52×4=622.080Mb/s、155.52×16=2488.32Mb/s、155.52×64=9953.28Mb/s。

依据 G.708 SDH 的 STM-0 网络节点接口。STM-0，速率为 51.840Mb/s；子 STM-11(sSTM-11)，速率为 2.2880Mb/s；sSTM-12，速率为 5.184Mb/s；sSTM-14，速率为 9.792Mb/s；sSTM-18，速率为 19.792Mb/s；sSTM-116，速率为 37.444Mb/s；sSTM-21，速率为 7.488Mb/s；sSTM-22，速率为 14.400Mb/s；sSTM-24 速率为 28.224Mb/s。

用 LAPS 的 IP over SDH 网络协议的配置如图 10.3 所示。

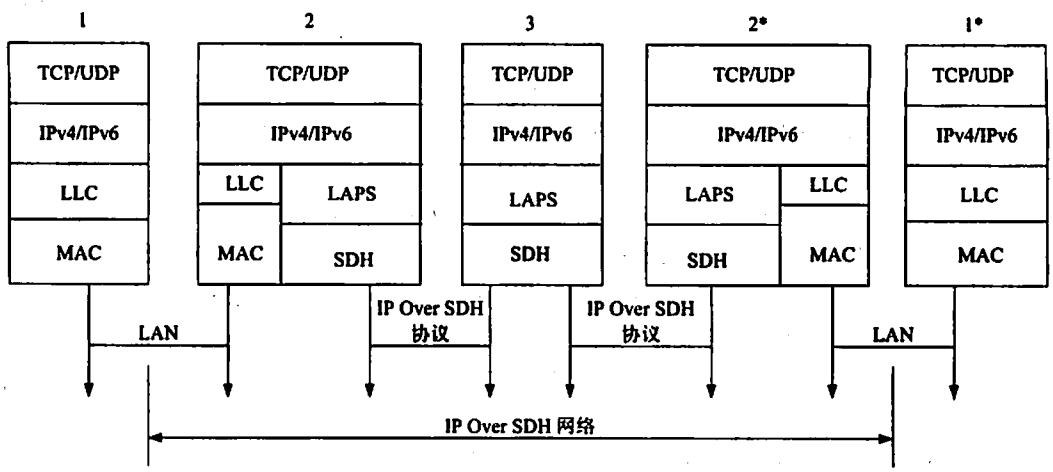


图 10.3 IP over SDH 网络协议的配置

图 10.3 中 1、1*为局域网工作站，2、2*为 IP over SDH 网络接入节点，3 为网络的核心节点。接入节点具有局域网协议与 IP over SDH 网络协议的转换功能。

10.3.1.2 IP over Optical

当前光纤技术迅猛发展，某些公司实验室的光纤系统容量已达 10.9Tb(波长数为 273，每一波长通道可达 40Gb)，所以当今骨干路由器采用称为 IP over WDM 或 IP over Optical 的技术将 IP 数据流直接在光通道上传输成为发展的方向。虽然点到点的 WDM 有巨大的宽带，但只提供传输带宽，还需要有灵活的光节点才能实现的高效的灵活组网能力，所以当今 IP over Optical 正在向其高端——由光核心网互联(光联网)的方向发展。因此 IP over Optical 又称光联网，备受设备制造商、电信运行商、标准制定机构，包括 ITU-T、IETF、ISO 等以及广大网络使用者关注。当今已提出一系列标准草案及部分标准文件。

下面介绍 IP over Optical 网络的构成及其工作原理。

1. IP over Optical 网络概述

IP over Optical 通过具有光接口的高速路由器直接在光上运行(直接接入到 WDM 光网上或直接接到光纤光上，核心网中间不经过 SDH/SONET 复用设备和 ATM 设备)。宏观地看，未来整个网络可以粗分为光传输网和业务网两大部分。光传输网由光交换机和 WDM 传输链路组成，负责高容量业务量的可靠传输并提供波长级流量工程的网络接口给业务平台。业务平台包括路由器、ATM 交换机和 ADM。业务平台完全依靠光传送平台提供波长通路来与对等层节点或网元实现连接。一个网络在总体功能上可以由数据(或传送)平面、控制平面、管理平面组成。控制平面主要涉及连接的建立以及支持这种连接所需要的处理，例如，路由域内邻居的发现/链路管理、信令、路由、寻址以及网络通道的提供和保护等。通常，控制平面主要是采用 IP 技术实施，管理平面为网络提供商与管理部门提供对网络与设备的管理。数据(或传送)平面用于传送与转发网内、网外客户的数据。显然，这 3 个平面是相互关联的。

任何网络都有控制机制。业界已对 IP over Optical 网络取得共识，即其控制机制应该利用 IP 协议，建立基于 IP 的控制平台。该平台的主要功能是要在光子网内和光子网间动态地提供和恢复光通道，以满足该网络开放多种业务，提供灵活的组网能力及调整网络规模。

光网络是由多个光子网组成，这些光子网是由不同的网络提供商经营的。光网络应该是智能化的，其智能化的最基本属性是网络的生存性，主要是网络出现故障时，要不中断通信的快速恢复机制，也就是保护机制。由于各种不同的信号，如语音、视频、数据、多媒体等对故障恢复时间的要求是不同的，所以这种保护机制要满足不同信号的需要，例如，可在第 2 层采用冗余的光系统或在第 3 层采用路由光层连接等措施。另外，还要考虑当光网络由多个光子网组成时的多供应商的各地子网之间的互操作性。

IP 在光网络上的传送主要涉及网络模型和各种接口，包括 IP 光接口、光子网间接口等，以及所用路由协议、路由及信令等。另外，还要考虑 IP 在光网络的 IP 光接口上期待开放的各种不同业务的特殊能力、业务模型等，以及网络互联。

2. IP over Optical 网络模型

IP over Optical 网络模型示意如图 10.4 所示。IP 网络通过用户网络接口(UNI)与光网络相连。IP 网络是由路由器实施互联，与光网络相连的路由器具有光接口，可直接与光网络相连，所以称该路由器为边缘路由器。光网络由多个光子网组成，光子网之间的接口为网络与网络接口(NNI)。光子网由多个光交叉连接设备(OXC)组成，它可以是全光型的 OXC，也可以是经光－电－光转换的 OXC。光子网之间的互联通过兼容的物理接口实现。其他形式的客户网络，例如，ATM 网、SDH 网等也可通过物理接口与光网络相连。

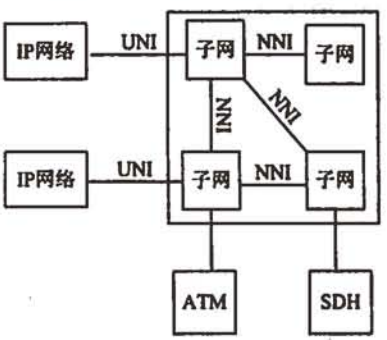


图 10.4　IP over Optical 网络模型示意图

光网络本身不能处理单个 IP 数据包，主要提供 IP 网及其他客户网络的光通道。光子网通过 OXC，而 OXC 之间有多条平行的光链路连接，从而形成全连接的网状网。通常光子网由同一生产 OXC 厂商的设备构成，或同一网络运营商组建(OXC 设备也是由同一生产厂商供应)，以便于管理、维护与运营。

当前，光交叉连接设备(OXC)是一个空分交换设备，它能交换一个光数据流从一个输入端口到一个输出端口。它可以是全光型的，也可以是在输入端口实施光－电转换，而在输出端口实施电－光转换，在 OXC 内部是电信号。一般一个 OXC 有控制平面处理器，实现在光网络中所需要的信令与路由协议。

OXC 把一个输入端口的信号交换到输出端口的功能是通过适当的配置交叉连接表实施的，该表列出全部输入端口与关联的输出端口条目，例如："条目<输入端口 i，输出端口

j>”，表示进入 i 端口的数据流将交换至输出端口 j。若一个光通道的建立要经过多个 OXC，那么各个 OXC 都要有相应的交叉连接，以便构成一条从最初的 OXC 的输入端口至远方的 OXC 的输出端口之间的物理光通道。必须指出，这里有一个前提条件，即光通道必须是双向的，也就是从输出端口至输入端口的返回路径与前向路径是相同的，都经过同样一组中间端口。

可以用 WDM 技术将 OXC 的多个数据流输出复用到一条光链路上。WDM 功能可以是单独的设备，也可以把 WDM 与 OXC 集成在一起。在后一种情况，交叉连接表为成对形式的条目。例如，“<{输入端口 i，波长 j}，{输出端口 k，波长 l}>”，表示在输入端口 i 的波长 j 上收到数据流，将其交换到输出端口 k 的波长 l 上。由以上讨论可知，光通道的自动建立涉及以合适的方式在相关的 OXC 中配置交叉连接表，以便获得所需的物理通道。

显然，在这种网络结构中，一对 IP 路由器在通信之前要先建立一条交换的光通道。这条光通道可能要经过多个光子网，在每个光子网中有不同的提供和恢复程序。对于基于 IP 的控制平面，需要设定标准的信令和路由协议，以便实现跨子网的端到端光通道的提供和恢复。与此类似，IP 在这种光网络上的传送，涉及确定 IP 的可达性和在光网络中无缝地建立 IP 端点之间的通道。

在 IP over Optical 网络模型示意图中有两种逻辑控制接口，即客户—光网络接口和光子网接口。这些接口称为用户—网络接口(UNI)和网络－网络接口(NNI)。两种接口的区别主要在于类型和控制流经过它们的数量。UNI 描述了客户和光网络之间的技术界限。经过 UNI 的控制与跨越该接口所规定的服务和该服务可以被访问的方式有关。由于光网络有一个基于 IP 的控制平台，所以有可能协调经过 UNI 和 NNI 的控制流程并且消除它们之间的差别。另一方面，可能需要尽量减少控制流量信息，特别是经过 UNI 的与路由相关的信息。

依据服务模型的不同，每种接口都可分为公用和专用两种。假如 UNI(或 NNI)是专用接口，那么路由信息(如拓扑状态信息)可以通过；如果 UNI(或 NNI)是公用接口，那么路由信息就不能通过，或是在明显限制(包括路由提取过滤等)下通过。由此，经过专用和公用逻辑接口可以有不同的关系存在(例如，对等模型和重叠模型)。实现这些逻辑接口的物理控制结构可以不同。例如，UNI 可以有直接接口、间接接口等。下面简单介绍一下直接接口。

直接接口是指如图 10.5 所示的一个边缘路由器与其连接的每个 OXC 之间存在一条带内或带外控制通路(IPCC)，该控制通路用于边缘路由器与 OXC 之间交换信令消息和路由消息。经过这个直接接口所交换的路由和信令信息的形式随服务定义而不同。路由协议可以是 OSPF/ISIS 或 BGP，也可以通过基于目录系统交换路由信息。信令协议可用 RSVP-TE 或 CR-LDP。

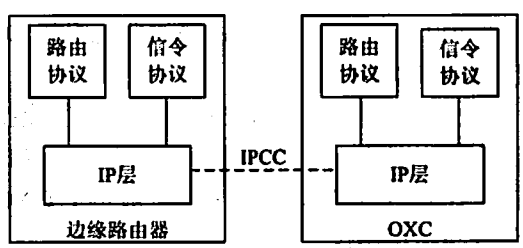


图 10.5 直接接口

10.3.1.3　IP over DWDM

目前的数据网络一般都采用多层结构，随着数据业务的井喷式发展，任何一层都可能限制网络的扩展能力，即多层结构的网络不能很好地满足今后数据业务的爆炸性增长。这就导致了网络结构从开销较大、功能重叠的多层协议结构向更紧密的 IP 直接到密集波分多路复用(Dense Wavelength Division Multiplexing，DWDM)的双层结构模型发展。

DWDM 技术之所以备受重视并得到广泛的应用，是因为 DWDM 系统具有以下特点：

- 使用 DWDM 技术，能很容易成倍地扩大系统的传输容量，DWDM 系统的总容量是不同波长信道传输容量之和，而且 DWDM 不改变原有的光纤设施。
- 光波分复用器是一种无源纤维光学器件，具有无电子电源、结构简单、体积小、重量轻、可靠性高等优点。
- 由于不同波长信道的光信号在同一根光纤独立传输，互不调制和干扰，因此能在一根光纤同时传输声音、视频、数据等多媒体信息，实现真正意义上的业务综合。
- DWDM 是未来全光网络的关键技术，所谓全光网络是指从传输、交换和处理都采用光学设备来实现，全光网络是未来信息高速公路的基础设施。
- 充分利用单模光纤的低损耗波段，增加光纤的传输容量，降低成本。目前，大多数光纤通信系统在一根光纤中只传输一个波长的信道，实际上光纤本身在长波长区域有很宽的低损耗区，可利用的波长有很多，潜力很大。利用 DWDM 技术可大大提高光纤传输带宽的利用率，使现有的光纤设施能得到充分的利用。

IP over DWDM 是目前最有发展前途的宽带网络技术，采用 DWDM 技术能极大地提高网络的带宽。IP over DWDM 代表了未来信息高速公路的发展方向，与 10 吉比特以太网相结合，将会对现有的网络技术产生难以估量的冲击。由于 IP over DWDM 在国际上研究才刚刚开始，其解决方案还不成熟，需要开发新的光纤传输接口，目前正由 ITU-TSGl5 和光互联网论坛(OIF)进行标准化工作，实验室内点到点最长的距离只能达到几百公里，因此，在数据通信高速发展的今天，IP over ATM 和 IP over SDH 仍会得到发展，其中核心骨干网将采用 IP over DWDM。

1. IP over DWDM 的优点

DWDM 作为新一代光纤通信支撑技术，不仅极大地拓展了光纤的带宽资源，使单纤传输容量增加几倍乃至几十倍，而且它对数据格式透明，可同时承载多种格式的业务信号，这使得把 IP 应用直接运行在光通道上(IP over DWDM)成为可能。IP over ATM、IP over SDH 和 IP over DWDM 的技术特点不同，应用范围不同，在网络中的作用也不尽相同，这形成了 IP 宽带网络技术中“三步曲”。目前，国外以 Web 业务为主的 IP 网络提供商主要使用 IP over SDH 的技术，而传统的电信运营商大多采用实时性要求高的业务，多选择 IP Over ATM，而 IP Over DWDM 技术是近年来随着 DWDM 进一步成熟而兴起的后起之秀，它将综合前两者的优点，使 IP 业务真正的运行在全光的环境中。

表 10.1 给出了 IP over ATM、IP over SDH 和 IP over DWDM 三种方案的多个性能参数的比较。传输链路的效率是线路传输的重要指标之一，从表 10.1 中可以看出，IP over ATM 由于要交“信元税”24%，因此传输效率很低，而 IP over SDH 取消了 ATM 层，提高效率 20%以上，这对带宽和价格昂贵的 WAN 来说是一个相当可观的数字。而 IP over DWDM

则去掉了 ATM 和 SDH 两层，省掉了很多开销，IP 数据包直接在光路上传输，大大提高了传输效率。原有的 SDH 用 TDM 技术挖掘带宽的潜力已几乎到了尽头，而只有 DWDM 才能解决提供高速带宽的难题。从结构上看 ATM 很复杂，而 DWDM 相对简单，在维护管理上，ATM 需要解决 IP 地址与 ATM 地址多重映射的矛盾，IP 网络的非连接特性与 ATM 面向连接之间的矛盾，使得网络管理维护比较复杂，IP over SDH 虽然省去了 ATM 层，但仍有较复杂的帧结构以及复用映射的问题，而 IP over DWDM 相比较而言，非常简单，是未来宽带 IP 网络的首选。过去曾一直认为，要保证 IP 网络应具有电话网络一样的可靠性和服务质量(QoS)，ATM/SDH 层必不可少，尤其是在数据业务流量不断增长的情况下。但 MPLS、流量工程和 QoS 等最新技术的出现和完善，通过在第三层合理设计网络结构，可获得同样级别的可靠性和服务质量保证。IP over DWDM 的全 IP 网络体系机构的骨干网可以提供极大的灵活性和无穷的增值服务开发的源泉，极大地提高电信运营商的新业务拓展能力，开放的结构使运营者可以自由选择实现各种类型网络的方法。

表 10.1 三种技术的比较

比较项目	IP over ATM	IP over SDH	IP over DWDM
效率	低	中	高
带宽	中	中	高
结构	复杂	略简	极简
价格	高	中	较低
传输性能	好	可以	好
维护管理	复杂	略简	简单

2. IP over DWDM 网络结构

IP over DWDM 网络有两种模式：层叠(overlay)模式和对等(peer)模式。

层叠模式的特点是：

- IP 路由器和建立在 DWDM 技术基础上光传送网(OTN)的 OXC 设备分别位于不同的管理域。
- IP 路由器与 OXC 设备以 UNI 接口连接，这意味着其中一方为客户方(IP 路由器)，另一方为网络提供服务(OXC)。
- IP 路由器并不知道 OTN 的拓扑，各个 IP 路由器根据自己与 OTN 提供和交换的 IP 网络拓扑信息构成邻接关系。
- IP 网络和 OTN 网络各自运行自己的信令和路由协议。
- IP 路由器可以向 OTN 提出请求以建立与其他 IP 路由器之间的光连接。

对等模式的特点是：

- IP 路由器和 OTN 上的 OXC 设备分别位于同一管理域。
- IP 路由器与 OXC 设备之间以 NNI 接口的方式相连，构成邻接关系并交换拓扑信息。
- IP 路由器和 OXC 设备一样，能知道域内的全部拓扑信息。
- IP 网络和 OTN 网络运行公共的信令和协议，使用相同的编址方案。
- IP 路由器请求与其他 IP 路由器之间的光连接。

ISP 可以根据自己的需要选择两种模式之一，如果希望保持 OTN 和 IP 网络分离并分别管理，可以选择层叠模式；如果需要统一管理 OTN 和 IP 网络，则选择对等模式。

IP over DWDM 的协议模型包括客户层(IP 层)协议、IP 适配协议、光通路协议以及 DWDM 光复用段和 DWDM 光传输段等。客户层协议包括 IPv4、IPv6 等协议。IP 适配层协议用于 IP 多协议封装、分组定界、差错检测以及 QoS 控制等功能。光通路协议包括数字客户适配和带宽管理(比特率和数据格式透明)、连接性证实等功能。光复用段功能包括带宽复用、线路故障分段和保护切换以及其他传送网维护功能。光传输段功能包括高速传输(色散补偿)、光放大器故障分析等功能。

10.3.2　典型例题分析

例 1　简述 IP over WDM 技术的基本原理及其主要器件。

分析：IP over WDM，也称光因特网或 IP 优化光互联网，是指省掉 ATM 层和 SDH 层，直接在光网上运行的因特网。它是一种由高性能 WDM 设备、吉比特和太比特路由交换机组成的数据通信网络，综合利用 IP 技术和基于 WDM 的光网络技术，交换机与路由器之间可通过光纤直接相连或连至光网络层。IP over WDM 充分利用 WDM 技术所带来的巨大传送带宽和高速路由交换机的强大交换能力，合理地在 IP 层与光学层之间实现流量工程、保护恢复、QoS 和网络管理等的优化配置，形成一种简单高效的网络体系结构。这里高性能网络路由器替代了传统的提供控制波长接入、交换、选路和保护倒换等功能的 ATM 和 SDH 交换和复用设备。光网络层(即服务层)可为包括 SDH 网元和网络互联设备在内的客户层设备提供波长路由。

IP over WDM 的基本工作原理是光纤直接与光耦合器相连，耦合器把各波长分开或组合，输入和输出端都用简单的光纤连接器。在发送端，将不同波长的光信号复用送入一根光纤中传输；在接收端，又将组合光信号解复用并送入不同的终端。因此，IP over WDM 是一个真正的链路层数据网，可以通过指定波长作旁路或直通连接，网络的业务工程可以只在 IP 层完成。由于使用了指定的波长，结构更灵活，并具有向光交换和全光选路结构转移的可能。由此可见，IP over WDM 是一种最直接、最简单、最经济的 IP 网络体系结构，非常适用于超大型 IP 骨干网。IP 和 DWDM 的结合，将出现一个全光 IP 网络。全光 IP 网络将按照 IP 技术和业务的特性进行优化，从而为 IP 网络乃至电信网络开辟一个新世界。

IP over WDM 网络的主要部件除了激光器、光纤、光放大器和光耦合器外，还包括光再生器、光转发器、光分插复用器(OADM)、光交叉连接器(OXC)和高速路由交换机。G.655 光纤因其色散的非线性效应小，最适合于 WDM 系统；高性能激光器是 WDM 系统中最昂贵的器件；光放大器主要采用掺铒光纤放大器 EDFA，可以同时放大 WDM 所有波长，但对平坦增益的要求较高；光耦合器用于将各波长组合在一起或分解开来，起复用和解复用作用；长途 WDM 系统中有电再生中继器，再生分 R1、R2 和 R3 三类；光转发器用于变换来自路由器或其他设备的光信号，并产生要插入光耦合器的正确波长光信号；光分插复用器和光交叉连接设备在长途 WDM 系统中运用较广泛；光交换机可使 ADM 和交叉连接设备作动态配置。

答案：略。

例 2 比较 IP over ATM 和 IP over SONET 两种组网方式。

分析：同步数字传送体系(SDH，Synchronous Digital Hierarchy)是国际电信联盟标准化部门(ITU-T，原国际电报电话咨询委员会 CCITT)于 1988 年接受 SONET 概念并经重新命名而提出的，它以同步复用、动态指针调整及组网灵活为特点，使欧洲、北美和日本三个地区性标准在 STM-1 等级达到统一；通过光接口标准化实现了多家厂商的产品横向兼容；通过丰富的开销比特提高了网络的 OAM 能力(诸如故障检测、端到端性能监视等)。另外，SDH 通过使用终端复用器(TM)、分插复用器(ADM)和数字交叉连接器(DXC)等网元，可非常方便灵活的组成线型、星型、环型等网络拓扑结构，上/下路灵活，并且网络自身具有很高的生存性(保护恢复和自愈能力很强)。

异步传递模式(ATM，Asynchronous Transfer Mode)是作为 B-ISDN 网络的最终解决方案而被 CCITT 提出的。它是通过固定长度的信元 Cell(53Bytes)以面向连接的方式工作的，不同种类的业务经过不同的 AAL 协议(AAL1、AAL3/4、AAL5)适配到 ATM 层，最后经过连接接纳控制 CAC(Connection Admition Control)和使用参数控制 UPC(Usage Parameter Control)来实现 ATM 网络业务接入和网络流量的管理与控制。IP over ATM 工作方式如下：IP 数据包在经 ATM 交换机或 ATM 路由器交换中转时，首先经地址解析协议 ARP 解析 IP 数据包包头，确定下一跳的 ATM 地址；然后，通过信令交换，建立 ATM 连接，再将 AAL 层数据经 SAR(Segmentation and Reassembly)装入信元 Cell，并加入相应的业务服务等级和参数控制；最后，在已建立的连接基础之上实现数据的安全快速传递、转换。

从以下六方面对 IP over ATM 和 IP over SONET 进行比较。

(1) 协议开销

到目前为止，ISP 考虑部署 IP over SONET 而不是 IP over ATM 的最大原因，是 ATM 信元包头(每 53 字节中有 5 个字节)导致的开销，有时称为信元税。AAL5(填充，8 字节报尾)和 LLC/SNAP 封装(8 字节)也增加了额外的开销。

在 ATM 上运行时，IP 只实现了大约 80%的可用线路速率，而在 SONET 上运行时，它可以实现 95%的线路速率。当昂贵的广域链路或受到带宽限制的其他链路用于主干路由器互联时，运行 IP over SONET 所增加的容量具有极大的吸引力。对带宽充足的环境，如局域网、带宽效率并不是太大的问题。

(2) 带宽管理

ATM 提供了全系列功能，可以管理为流经一条链路的各条信息流(VCC)分配的带宽。它根据要求的服务质量，为这些 VCC 分配灵活的带宽。由于其信元交换特点，ATM 允许多条信息流同时共享同一条链路，并保障为每条信息流分配一定数量的带宽。而 PPP 则没有提供任何带宽管理功能。它提供了一条简单的点到点链路，IP 层必须调度其分组传输，保证每条信息流获得公平的链路带宽份额。在速度慢的链路上可能会出现问题，因为在这些链路上，属于优先级低的信息流的大型分组传输，可能会堵住其他优先级高的分组传输。

(3) 服务质量

服务质量(QoS)与端到端分组延迟、抖动、丢包和吞吐量等参数有关。ATM 提供了一套丰富的可以针对每条 VCC 协商确定的 QoS 参数。交换机中的智能排队和调度机制保证了可以提供协商的 QoS。ATM 提供了各种服务等级，可以满足不同的应用要求。例如，具有非常特殊的 QoS 要求的应用，可以使用恒定比特率(CBR)或可变比特率(VBR)服务。而

要求具有弹性特点的应用则可以使用可用比特率(ABR)或未指定比特率(UBR)服务。这些本机 ATM 功能允许在 IP 层简便地提供 QoS，在 IP 层，具有特定 QoS 要求的每条信息流都可以映射到自己的具有特定 QoS 的 VCC 上。例如：语音流可以映射到实时 CBR 或 VBR 连接上，而文件传输可以映射到 ABR 连接上。PPP 在单一的点到点链路上运行，不提供任何 QoS 功能。如前所述，IP 层必须智能化地管理其分组传输，以保证为信息流提供适当的 QoS。尽管 ATM 提供了丰富的 QoS 参数集，基于 QoS 的服务限定于连接两台路由器的 ATM 路径。为了向 IP 分组提供端到端 QoS，路由器还必须提供智能排队和调度机制。从这个意义上看，当 IP 网络重叠在 ATM 网络顶部时，路由器把 ATM 连接视为点到点链路，这与 PPP 相类似，尽管实际通信可能会发生在由 ATM 交换机组成的网络上。

(4) 地址和路由

ATM 被定义成完整的网络层，它为末端系统寻址和连接路由提供了广泛的功能。ATM 网络可以跨越巨大的地理区域，在路由器之间提供了通用的互联机制，而不管这些路由器位于什么位置。相比之下，PPP 仅在直接的点到点链路上运行，没有寻址或路由功能。为了创建主干网络，必须在主干路由器之间开通点到点链路。必须开通多条链路，以实现链路的容错性。在某些情况下，可能需要配置全网状结构，以使跨越主干所需的站数达到最小。全网状结构不仅成本很高，而且可能并不可行，因为在广域中连接纯 SONET 链路的通路有限。在与 SVC 配合使用时，ATM 在路由器之间实现了任意路由器连接，而不需配置全网状结构。即使 ATM 网络中的某些链路出现故障，动态 SVC 路由功能仍可以发现迂回路由，而一直确保任何两台路由器之间的连接。ATM 最有用的功能是，运营商可以在一个 ATM 接口上，简便地建立与其他路由器的连接。在主干路由器网络中，大多数路由器将需要互相通信，这意味着最终将需要全网状连接，而不管采用的是点到点链路还是 SVC。但是，ATM 还可以实现更加灵活的网络工程设计能力，因为它能够在不同的链路上路由 SVC，并能够通过相同的接入链路，把一台路由器连接到多个信宿上。ATM 流量控制协议采用多种功能，如呼叫接纳控制 CAC、通信整形和用户参数控制 UPC 或策略制订，确保信息流一直位于协商的通信合同的边界之内。超过的通信将打上标记，可以在网络过载时丢掉这些分组。因此最终用户可以根据带标记的分组或丢掉的分组，了解与拥塞有关的隐含信息。ATM 的信元级丢弃与 TCP 的分组级流量控制交互能力较差，为了尽量消除这一问题，业内已经为 ATM 开发了多种挂接技术，如部分丢包 PPD 或早期丢包 EPD，以识别分组 AAL 帧边界，在过载情况下丢掉整个帧。PPP 没有提供流量控制机制，因此 TCP 的流量控制直接在 PPP 链路上运行。如前所述，不管路由器是通过 ATM 相连还是直接通过 SONET 相连，路由器都查看彼此之间的(一定带宽)管道，必须采用适当的缓冲机制，以确保合理的吞吐量。

(5) 多协议封装

ATM 为多种协议共享同一链路提供了两种机制。第一种机制称为 VCC 多路复用，这种机制将每种协议分配给各个 VCC、ATM 层多路复用及反多路复用 VCC，因此用户不需增加任何其他封装包头来区别各种协议。第二种机制称为 LLC 多路复用，这种机制允许多种协议共享同一个 VCC。它在每个分组中增加一个 8 字节封装包头，以鉴别它属于哪个协议。当可用的 VCC 数量有限，且在各种协议之间共享 VCC 时，可以使用这种形式的多路复用。PPP 提供了一种类似于 ATM 中 LLC 多路复用的多协议封装形式。它采用 1 字节或

2字节协议标识符字段作为封装包头。在最主要的方面，PPP和ATM的多协议封装功能是同等的。

(6) 容错

通过使用一种动态路由协议(称为专用网络节点接口 PNNI 协议)，在发生故障的链路和交换机周围路由连接，ATM 提供了故障恢复能力。目前，PNNI 只在建立初始连接过程中提供迂回路由功能。PPP 没有任何容错功能，因为它在单一链路上运行。但是，底层 SONET 层提供了内置的保护功能，在运行光环发生故障时，可以把交换机切换到迂回光环上；当在 SONET 上运行时，还可以在 ATM 上应用这一功能。

答案：略。

例3 什么是 IP over SDH?

分析：详见 10.3.1.1 节。

答案：所谓 IP over SDH，即以 IP over SDH 网络作为 IP 数据网络的物理传输网络，并使用链路适配及成帧协议(PPP)对 IP 数据包进行封装，然后按字节同步的方式把封装后的 IP 数据包映射到 SDH 的同步净荷封装(SPE)中，按其各次群相应的线速率进行连续传输。

例4 列举解决 IP over WDM 网络路由问题的两种方式。

分析：分离路由方式(separated routing solution)，IP 网络和 WDM 网络仍使用各自的路由机制，即 IP 网络使用传统的动态路由协议(OSPF，BGP 等)路由 IP 分组，如果 IP 网络使用了后面提到的 MPLS 技术也可以使用与之相关的协议，WDM 网络则使用路由和波长分配(routing and wavelength assignment，RWA)算法为光路确定路由和波长，两者互不干扰。

整合路由方式(integrated routing solution)，IP 网络和 WDM 网络使用统一的路由机制，IP 路由器在确定路由时应能知道 WDM 网络甚至物理网络的参数信息。使用整合路由方式对 OADM、OXC 等器件的要求也更苛刻了，因为虚拓扑的改变可能相当频繁，不像目前的 WDM 传送网，虚拓扑是在相对较长时间内缓慢变化的。

答案：分离路由方式、整合路由方式。

10.3.3 同步练习

1. 讨论 IP over DWDM 网络的两种模式及各自特点。
2. 简述 IP over SDH 技术的优劣点。
3. 简述 IP over SDH 与路由器的关系。

10.3.4 同步练习参考答案

1. IP over DWDM 网络有两种模式：层叠(overlay)模式和对等(peer)模式。详见 10.3.1.2 节。

2. IP over SDH 相对于 IP over ATM 传输方式具有更高的传输效率，更适合于组建专门承载 IP 业务的数据网络。其主要优点为：

- IP 数据包通过 PPP 协议直接映射到 SDH 帧结构上，省去中间的 ATM 层，简化了 IP 网络体系结构，提高数据传输效率。
- 将 IP 网络技术建立在 SDH 传输平台上，可以很容易地跨越地区和国界，兼容各种不同的技术和标准，实现网络互联。
- 可以充分利用 SDH 技术的各种优点(如：自动保护切换 APS)保证网络的可靠性。
- 有利于实施 IP 多点广播技术(IP Multicasting)。
- 适用于 IP 骨干网。

但是，IP over SDH 技术仍具有以下不足之处：

- 不适于集数据、语音、图像等的多业务平台。
- 目前 IP over SDH 技术一般可进行业务分级(CoS)，尚不能像 IP over ATM 技术那样提供较好的服务质量(QoS)。
- 对大规模的网络，需处理庞大、复杂的路由表，而且路由表查找困难，路由信息占用较大的带宽。
- 尚不支持虚拟专用网(VPN)和电路仿真。
- 网络扩充性能较差，不如 IP over ATM 技术那样灵活。

3. IP over SDH 技术的实现需要高速路由器和 PPP 协议，采用的仍然是传统路由器的逐包转发方式。其基本思路是将路由计算与包的转发分开，采用缓冲技术、硬件芯片快速处理技术、以 ATM 信元交换矩阵作为路由器内部体系构架的交换路由技术，将路由器包的逐包转发速度控制到与第二层交换的速度相当。它无须利用广域网上的 ATM 交换机来建立虚电路 VC。

为保证路由与 SDH 设备之间的互操作性，路由器卡应支持下述 SDH 开销字节功能：

- 用于自动保护切换(APS)的 K1、K2 字节，允许路由器与路由器之间、路由器与 ADM 之间进行切换。
- 通过踪迹字节(J1)可由路由器卡来插入和监视。
- 差错监视字节(B1、B2 和 B3)、复用段远端差错指示字节(M1)和通道状态字节(G1)可由路由器来插入和监视。
- 路由器应对 SDH 的段、线路和通道进行报警和性能监视。
- 路由器卡从 SDH 系统提取要定时。

IP over SDH 中以链路方式来支付 Internet 网络，不能参与 Internet 网络的寻址。它的作用是将路由器以点到点的方式连接起来，提高点到点之间的传输速率。它并没有从总体上提高 Internet 网络的性能，这种 Internet 网络本质上仍是一个路由器网。Internet 网络整体性能的提高将取决于路由器技术是否有突破性进展。

目前不少网络设备公司已推出基于 IP over SDH 技术的交换路由器产品，如 Cisco 千兆位交换路由器 GSR12000、Ascend，千兆位路由转发器 GRF、Lucent，于 1998 年推出的 Packet-star 千兆位路由器等。这些设备在交换功能方面引入了 ATM 技术，与传统路由器相比，在技术方向有了重大突破，表现在吞吐量大(达 60Gb/s)和传送时延小(14μs~40μs)，为 IP over SDH 的实现奠定了基础。但是，千兆比特高速路由器在实现第 2 层交换与第 3 层选路的综合的同时，也带来了设备的复杂性。此外，这种突破性技术尚不能广泛应用于普通路由器。因而除非网络上的全部路由器都能采用千兆比特速路由器技术，否则仍难以从整体上提高

Internet 网络的水平。所以，IP over SDH 主要用于在干线上疏导高速率数据流。

10.4 通 信 服 务

10.4.1 考点辅导

10.4.1.1 DDN

1. 什么是 DDN

数字数据网(Digital Data Network)是利用数字信道传输数据信号的数据传输网，它的传输媒介有光缆、数字微波、卫星信道以及用户端可用的普通电缆和双绞线。利用数字信道传输数据信号与传统的模拟信道相比，具有传输质量高、速度快、带宽利用率高等一系列优点。DDN 向用户提供的是半永久性的数字连接，沿途不进行复杂的软件处理，因此延时较短，避免了分组网中传输时延大且不固定的缺点；DDN 采用交叉连接装置，可根据用户需要，在约定的时间内接通所需带宽的线路，信道容量的分配和接续在计算机控制下进行，具有极大的灵活性，使用户可以开通种类繁多的信息业务，传输任何合适的信息。

DDN 是目前电信部门向用户提供的一种高速通信业务。从技术上看，DDN 的原理与 SDH 非常相似，也是将多路复用技术应用于数字传输信道，来支持多个用户“共享”通信资源，只不过它所定义的速率较低。从用户的观点来看，DDN 仅是一条支持用户数据点到点高速传输的通道。由于 DDN 采用时分多路复用技术，将支持数字信息高速传输的光纤通道划分为一系列的子信道(例如，2.048Mb/s 的光纤信道划分为 32 路 64Kb/s 的子信道，可以分配给 32 个用户使用)，因此用户可以向电信部门定时的租用子信道以支持自己的应用，并且在用户租用的时间周期内，整个子信道的资源归用户“所有”，不允许其他用户使用这个子信道，即使本用户并没有数据传输的要求。由于不同的用户对于数据传输的速率要求不同(DDN 的基本速率为 64Kb/s)，因此用户租用的信道速率应为 64Kb/s 的整数倍。需要注意的是，DDN 本身并不提供任何通信协议的支持，在 DDN 信道上使用何种通信协议由用户自行决定，例如，可以仍然使用 X.25 协议或者帧中继协议。

2. DDN 网的特点

DDN 网具有以下的特点：

- 传输速率高　在 DDN 网内的数字交叉连接复用设备能提供 2Mb/s 或 N×64Kb/s(≤2Mb/s)速率的数字传输信道。
- 传输质量较高　数字中继大量采用光纤传输系统，用户之间专有固定连接，网络时延小。
- 协议简单　采用交叉连接技术和时分复用技术，由智能化程度较高的用户端设备来完成协议的转换，本身不受任何规程的约束，是全透明网，面向各类数据用户。
- 灵活的连接方式　可以支持数据、语音、图像传输等多种业务，它不仅可以和用户终端设备进行连接，也可以和用户网络连接，为用户提供灵活的组网环境。
- 电路可靠性高　采用路由迂回和备用方式，使电路安全可靠。

- 网络运行管理简便　采用网管对网络业务进行调度监控，业务生成迅速。

3. 节点类型

在“中国 DDN 技术体制”中将 DDN 节点分成 2 兆节点、接入节点和用户节点三种类型。

(1) 2 兆节点

2 兆节点是 DDN 网络的骨干节点，执行网络业务的转换功能。主要提供 2048Kb/s(E1)数字通道的接口和交叉连接、对 N×64Kb/s 电路进行复用和交叉连接以及帧中继业务的转接功能。

(2) 接入节点

接入节点主要为 DDN 各类业务提供接入功能，主要有：

- N×64 Kb/s、2048Kb/s 数字通道的接口。
- N×64 Kb/s(N=1~31)的复用。
- 小于 64 Kb/s 子速率复用和交叉连接。
- 帧中继业务用户接入和本地帧中继功能。
- 压缩语音/G3 传真用户入网。

(3) 用户节点

用户节点主要为 DDN 用户入网提供接口并进行必要的协议转换。它包括小容量时分复用设备；LAN 通过帧中继互联的网桥/路由器等。

在实际组建各级网络时，可以根据网络规模、业务量等具体情况，酌情变动上述节点类型的划分。例如，把 2 兆节点和接入节点归并为一类节点，或者把接入节点和用户节点归并为一类节点，以满足具体情况下的需要。

10.4.1.2　NAT

NAT 英文全称是 Network Address Translation，中文意思是“网络地址转换”。它是一个 IETF 标准，允许一个机构以一个公用 IP(Internet Protocol)地址出现在 Internet 上。顾名思义，它是一种把内部私有网络地址(IP 地址)转换成合法网络 IP 地址的技术。

简单的说，NAT 就是在局域网内部网络中使用内部地址，而当内部节点要与外部网络进行通信时，就在网关处，将内部地址替换成公用地址，从而在外部公网(Internet)上正常使用，NAT 可以使多台计算机共享 Internet 连接，这一功能很好地解决了公共 IP 地址紧缺的问题。通过这种方法，您可以只申请一个合法 IP 地址，就把整个局域网中的计算机接入 Internet 中。这时，NAT 屏蔽了内部网络，所有内部网计算机对于公共网络来说是不可见的，而内部网计算机用户通常不会意识到 NAT 的存在。这里提到的内部地址，是指在内部网络中分配给节点的私有 IP 地址，这个地址只能在内部网络中使用，不能被路由。虽然内部地址可以随机挑选，但是通常使用的是下面的地址：10.0.0.0~10.255.255.255，172.16.0.0~172.16.255.255，192.168.0.0~192.168.255.255。NAT 将这些无法在互联网上使用的保留 IP 地址转换成可以在互联网上使用的合法 IP 地址。而全局地址，是指合法的 IP 地址，是由 NIC(网络信息中心)或者 ISP(网络服务提供商)分配的地址，对外代表一个或多个内部局部地址，是全球统一的可寻址的地址。

NAT 功能通常被集成到路由器、防火墙、ISDN 路由器或者单独的 NAT 设备中。譬如，

Cisco 路由器中已经加入这一功能，网络管理员只需在路由器的 IOS 中设置 NAT 功能，就可以实现对内部网络的屏蔽。再譬如，防火墙将 Web Server 的内部地址 192.168.1.1 映射为外部地址 202.196.23.21，外部访问 202.196.23.21 地址实际上就是访问 192.168.1.1。对于资金有限的小型企业来说，现在通过软件也可以实现这一功能。Windows 98 SE、Windows 2000 都包含了这一功能。

NAT 有三种类型：静态 NAT(Static NAT)、动态地址 NAT(Pooled NAT)、网络地址端口转换 NAPT(Network Address Port Translation，Port-Level NAT)。

其中静态 NAT 设置起来最为简单是最容易实现的一种类型，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。而动态地址 NAT 则是在外部网络中定义了一系列的合法地址，采用动态分配的方法映射到内部网络。NAPT 则是把内部地址映射到外部网络的一个 IP 地址的不同端口上。根据不同的需要，三种 NAT 方案各有利弊。

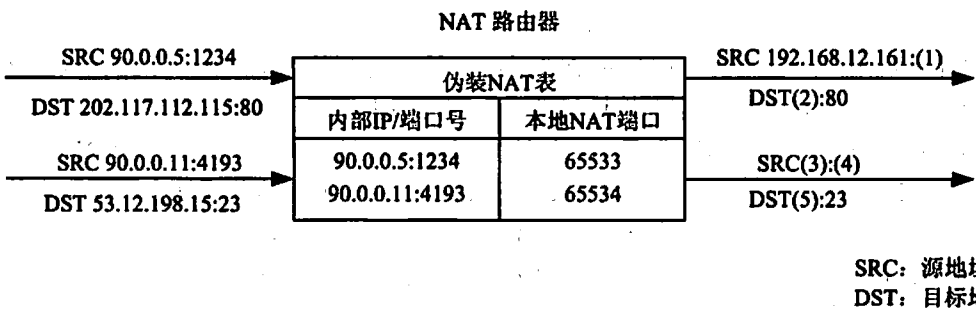
动态地址 NAT 只是转换 IP 地址，它为每一个内部的 IP 地址分配一个临时的外部 IP 地址，主要应用于拨号，对于频繁的远程连接也可以采用动态 NAT。当远程用户连接上之后，动态地址 NAT 就会分配给它一个 IP 地址，用户断开时，这个 IP 地址就会被释放而留待以后使用。

网络地址端口转换 NAPT 是人们比较熟悉的一种转换方式。NAPT 普遍应用在接入设备中，它可以将中小型的网络隐藏在一个合法的 IP 地址后面。NAPT 与动态地址 NAT 不同，它将内部连接映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加上一个由 NAT 设备选定的 TCP 端口号。

在 Internet 中使用 NAPT 时，所有不同的信息流看起来好像来源于同一个 IP 地址。这个优点在小型办公室内非常实用，通过从 ISP 处申请一个 IP 地址，将多个连接通过 NAPT 接入 Internet。实际上，许多 SOHO 远程访问设备支持基于 PPP 的动态 IP 地址。这样，ISP 甚至不需要支持 NAPT，就可以做到多个内部 IP 地址共用一个外部 IP 地址连接上 Internet。虽然这样会导致信道的一定拥塞，但考虑到节省的 ISP 上网费用和易管理的特点，用 NAPT 还是很值得的。

10.4.2 典型例题分析

例 1 NAT 中的动态地址翻译和 IP 地址伪装有什么区别？下图是某个路由器上的地址伪装表，将图中(1)~(5)处空缺的信息填写在相应位置。(2004 年下半年下午试题四)



分析：根据 IP 地址伪装的定义可知，经过 NAT 路由器的地址转换后内部地址映射到外部网络中的一个单独的 IP 地址上，因此(3)空应为 192.168.12.161。同时映射后的地址上要加上由 NAT 路由器选定的 TCP 端口号，因此(1)空应为 65533，(4)空应为 65534。IP 地址伪装的过程并不改变 IP 包中的目标地址，因此(2)空应为 202.117.112.115，(5)空应为 53.12.198.15。

答案：动态地址翻译，即动态地址 NAT(Pooled NAT)，是在外部网络中定义了一系列的合法地址，采用动态分配的方法映射到内部网络。而 IP 地址伪装，即网络地址端口转换 NAPT(Network Address Port Translation，Port-Level NAT)，则是把内部地址映射到外部网络的一个 IP 地址的不同端口上，它将内部连接映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加上一个由 NAT 设备选定的 TCP 端口号。

(1) 65533
(2) 202.117.112.115
(3) 192.168.12.161
(4) 65534
(5) 53.12.198.15

例 2　在我国的技术体制中，DDN 有哪三种节点类型？

分析：详见 10.4.1.1 节。

答案：2 兆节点、接入节点、用户节点。

例 3　NAT 转换中使用的地址有哪四类？

分析：NAT 转换中使用的地址有以下四类：

内部局部地址——对网络内部的主机而言，IP 地址是惟一的，但该地址并不具有全局意义。

内部全局地址——由 IANA 或服务提供商分配的 IP 地址，它们在全局地址空间或互联网上是合法的。内部局部地址转换为内部全局地址，并为互联网所用。

外部局部地址——外部网络中主机的 IP 地址，代表内部网络，并在本地网中是合法的，这些地址不一定有全局意义。

外部全局地址——在 Internet 空间中全球可路由的 IP 地址。

答案：内部局部地址、内部全局地址、外部局部地址和外部全局地址。

10.4.3　同步练习

1. 简述 DDN 技术。
2. 简述 DDN 的主要特点。
3. 网络地址转换有哪几种类型？

10.4.4　同步练习参考答案

1. DDN 是利用数字信道传输数据信号的数据传输网。它的主要作用是向用户提供永

久性和半永久性连接的数字数据传输信道，既可用于计算机之间的通信，也可用于传送数字化传真、数字语音、数字图像信号或其他数字化信号。永久性连接的数字数据传输信道是指用户间建立固定连接，传输速率不变的独占带宽电路。半永久性连接的数字数据传输信道对用户来说是非交换性的。

2. 传输速率高、传输质量较高、协议简单、灵活的连接方式、电路可靠性高、网络运行管理简便。

3. 网络地址转换(NAT)有三种类型：静态 NAT(Static NAT)、动态地址 NAT(Pooled NAT)、网络地址端口转换 NAPT(Network Address Port Translation，Port-Level NAT)。

10.5 网 络 管 理

10.5.1 考点辅导

10.5.1.1 基于 TMN 的网络管理

电信网络管理的目标是要最大限度地利用电信网络资源，提高网络的运行质量和效率，向用户提供良好的通信服务。而电信管理网(TMN)则正是为电信网络管理目标的实现提供了一套整体解决方案，它能简化多厂商混合网络环境下电信运营企业的管理模式，降低电信运营的管理成本，从而使企业获得更好的效益。

1. 什么是 TMN

国际电信联盟(ITU)在 M.3010 建议中指出，电信管理网的基本概念是提供一个有组织的网络结构，以取得各种类型的操作系统之间，操作系统与电信设备之间的互联。它是采用商定的具有标准协议和信息的接口进行管理信息交换的体系结构。提出 TMN 体系结构的目的是支撑电信网和电信业务的规划、配置、安装、操作及组织。

TMN 应用领域非常广泛，涉及电信网及电信业务管理的许多方面，从业务预测到网络规划；从电信工程、系统安装到运行维护、网络组织；从业务控制和质量保证到电信企业的事物管理，都是它的应用范围。下面是 TMN 管理比较典型的电信设备例子：公用网和专用网(包括 ISDN，移动网，专用语音网，虚拟专用网，智能网)、TMN 本身、传输终端(复用器，交叉连接，通道变频设备，ADM 等)、数字和模拟传输系统(电缆，光纤，无线，卫星等)、恢复系统、数字和模拟交换机、(计算机主机，前端处理器，集群控制器，文件服务器)、电路交换及分组交换、信令终端和系统(SP，STP，实时数据库)、承载业务及电信业务、PBXS，PBX 接入及用户终端、ISDN 用户终端、相关的支持系统(如数字同步网)。

2. TMN 的管理业务和管理功能

TMN 管理业务是从使用者的角度来描述的对电信网的操作、组织与维护的管理活动。TMN 管理业务基本可以归纳为以下 3 类：

- 通信网日常业务和网络运行管理业务。
- 通信网的检测、测试和故障处理等网络维护管理业务。
- 网络控制和异常业务处理等网络控制业务。

TMN 的用户可以是电信运营公司，电信运营公司的管理组织部门，维护部门及人员，也可以是电信业务所服务的客户。

TMN 的各类管理功能支持 TMN 的管理业务的实现，满足对被管理网络的操作、维护和管理的需要。管理人员通过人机接口与管理应用交互，通过 TMN 提供的管理功能对被管理网络进行各项管理操作活动。TMN 为电信网及电信业务提供一系列的管理功能，主要划分为以下 5 种管理功能域：

(1) 性能管理(Performance Management)

性能管理是对电信设备的性能和网络单元的有效性进行评估，并提出评价报告的一组功能。包括性能测试、性能分析及性能控制。

(2) 配置管理(Configuration Management)

配置管理功能包括提供状态和控制及安装功能。对网络单元的配置，业务的投入，开/停业务等进行管理，对网络的状态进行管理。

(3) 账务管理(Accounting Management)

账务管理功能测试电信网中各种业务的使用情况，计算处理使用电信业务的应收费用，并对电信业务的收费过程提供支持。

(4) 故障管理(Fault Management)

故障管理功能是对电信网的运行情况异常和设备安装环境异常进行管理，对网络的状态进行管理。

(5) 安全管理(Security Management)

安全管理主要提供对网络及网络设备进行安全保护的能力。主要有接入及用户权限的管理，安全审查及安全报警处理。

TMN 的功能可以划分为不同的层次由高到低依次为：

(1) 事务管理层

事务管理层是最高的管理功能层。该层负责设定目标任务，但不管具体目标的实现，通常需要管理人员的介入。

(2) 服务管理层

服务管理层主要处理网络提供的服务相关事项。诸如，提供用户与网络运营者之间的接口，与事务管理层及网络管理层的交互等。

(3) 网络管理层

网络管理层对所辖区域内的所有网元进行管理，主要的功能包括：从全网的观点协调与控制所有网元的活动；提供、修改或终止网络服务；就网络性能、可用性等事项与上面的服务管理层进行交互。

(4) 单元管理层

单元管理层直接行使对个别网元的管理职能，主要的功能包括：控制与协调一系列网络单元；为网络层的管理与网络单元进行通信提供协调功能；维护与网络单元有关的统计等数据。

3. TMN 的标准化协议

TMN 的最主要的标准之一是 ITU-T M.3010，它是关于 TMN 的总体要求，涉及总体原则、体系结构、逻辑分层结构及基本功能要求。M.3400 是关于 TMN 的管理功能的标准。

M.3200 系列是关于 TMN 的管理业务及各种电信网上的 TMN 管理业务标准。M.3020 是 TMN 的接口规范定义方法。M.3100 系列是 TMN 的通用管理信息模型。

4. TMN 的体系结构

下面将介绍 TMN 的功能体系结构和信息体系结构，以及 TMN 提供的四种接口。

(1) TMN 的功能体系结构

在 TMN 的功能体系结构中，引入了一组标准的功能块(function block)和有可能发生信息交换的参考点。TMN 的功能模型中包括操作系统的功能(OSF)，各种中介功能(MF)，适配器功能(OAF)。另外，TMN 也连到各网络单元功能(NEF)和各工作站(WSF)。有些功能部分属于 TMN 范畴，部分在 TMN 范畴外。功能体系结构中的参考点(reference point)是指两个非重叠的功能连接处的概念点，通过它来识别在这些功能之间交互的信息类型。在 TMN 中，为了描述各功能之间的关系，引入了参考点 q、f、x，另外 TMN 与外界相关的参考点为 g、m。q 参考点在 OSF 与 OSF 之间、OSF 与 MF 之间、OSF 与 NEF 之间、MF 与 MF 之间。f 参考点在 OSF 与 WSF 之间、WSF 与 MF 之间。x 参考点在 OSF 与其他 TMN 的 OSF 之间。m 参考点在非 TMN 标准网元(或 OSF)与 QAF 之间。g 参考点在 WSF 与用户之间。TMN 管理分层模型与功能块的关系：

- OSF 功能块处理与电信管理相关的信息，支持和控制电信管理功能的实现。对应 TMN 的管理分层又可分为行业管理 OSF、业务管理 OSF、网络管理 OSF 和基本 OSF。
- 中介功能 MF，在 OSF 与 NEF(或 QAF)之间进行信息的传送，以保证各功能块对信息模式的需求，并使网元(NE)到 OSF 的结构更加灵活。
- 数据通信功能 DCF，提供各功能块之间数据通信的方法。提供 OSI 参考模型中第一层到第三层的功能。
- 网元功能块 NEF，在网元中，网元为了被管理而向 TMN 描述其通信功能是网元功能 NEF 的一部分，这部分属于 TMN，而 NEF 的其他功能则在 TMN 之外。
- 适配器功能(WSF)提供 TMN 与用户之间的交互能力，而人机界面则属于 TMN 之外。

(2) TMN 的信息体系结构

TMN 的信息体系结构应用 OSI 系统管理的原则，引入了管理者和代理(Manager/Agent)的概念，强调在面向事务处理(Transaction-Oriented)的信息交换中采用面向对象(Object-Oriented)的技术。主要包括管理信息模型及管理信息交换两个方面。管理信息模型是对网络资源及其所支持的管理活动的抽象表示。在信息模型中，网络资源被抽象为被管理的对象(Managed Object)。模型决定了以标准方式进行信息交换的范围，模型中的活动(Activity)实现了 TMN 的各种管理操作，如信息的存储、提取与处理。管理信息交换涉及 TMN 的数据通信功能 DCF 和消息传递功能 MCF，主要是接口规范及协议栈。电信管理是一种信息处理的过程，每一种特定的管理应用，按照 ITU-T X.701 建议中系统管理模型(System Management Model)中的定义，都具有管理者、代理者两方面的作用。在管理者/代理者面前，网络资源是一棵信息树(Information Tree)，即被管理对象信息库(MIB，Management Information Base)。代理者(Agent)直接操作被管理资源，管理者(Manager)通过 CMIS(Common Management Information Service)实施管理操纵。

(3) TMN 的接口

在 TMN 的体系结构可以看出，在 TMN 中共有四种接口，即 Qx、Q3、X、F。

① Q3 接口

目前的标准化主要集中在 Q3 接口上，Q3 接口与通常谈到的接口很不同，比如一个 RS232 接口等，都是比较单一的通信接口，而 Q3 接口是一个集合，而且是跨越了整个 OSIQ 七层模型的协议集合。从第一层到第三层的 Q3 接口协议标准是 Q.811，称之为低层协议栈。从第四层到第七层的 Q3 接口协议标准是 Q.812，称之为高层协议。Q.811/Q.812 适用于任何一种 Q3 接口。Q.812 中最上层的两个协议是 CMIP 与 FTAM，前者用于面向事务处理的管理应用，后者用于面向文件传输的文件传送、接入与管理。在这里还要特别指出，Q3 接口不仅包括在第七层中用到的管理信息和管理信息模型(MIB)，在通信协议 Q.811/812 之上还要有 G.774 和 M.3100。M.3100 是面向网元的通用信息模型。G.774 是 SDH 的管理信息模型。Q.821，Q.822 是 Q3 接口中关于报警和性能管理的支持对象定义。

② Qx 接口

在管理系统的实施中，很多产品采用 Qx 接口作为向 Q3 接口的过渡。Q3 接口连接 OS 与 OS，OS 与 MD，OS 与 QA。Qx 是不完善的 Q3 接口，Qx 很像 Q3，但功能不完善，处于成本和效率方面的考虑，它取舍了 Q3 中的某些部分，但是 Q3 的哪些部分可以被去掉并没有标准，因此往往是非标准厂家的 Q 接口。Qx 与 Q3 有两点不同之处：一是参考点不同；二是所承载的信息不同。

③ F 接口

F 接口处于工作站(WS)与具有 OSF、MF 功能的物理构件之间(如 WS 与 MD)。它将 TMN 的管理功能呈现给管理者，或将管理者的干预转呈给管理系统，解决与 TMN 的五大管理功能领域相关的人机接口的支持能力，使管理者通过电信管理网(TMN)接入电信管理系统。人机接口(HMI)使管理者与系统之间交换信息。管理者与控制系统的交互是基于输入/输出、特殊动作和人机对话处理等各种交互机制。

④ X 接口

X 接口提供 TMN 与 TMN 之间或 TMN 与具有 TMN 接口的其他管理网络之间的连接。在这种情况下，相对 Q 接口而言，X 接口上需要更强的安全管理能力，要对 TMN 外部实体访问信息模型设置更多的限制。为了引入安全等级，防止不诚实的否认等，也需要附加的协议，但 X 接口应用层协议与 Q3 的是一致的。

10.5.1.2　基于 CORBA 的网络管理

1. 基于 CORBA 技术的有关网管标准

与 CORBA 有关的基础标准分别是 X.780、X.780.1、Q.816、Q.816.1、M.3120、Q.821.1、Q.821.1 和 X.781，与这些基础标准相关的标准还有 M.3010、M.3013、M.3100、M.3020、X.721、Q.822、X.739 和 Q.821。

2000 年版的 M.3010 和 M.3013 为 CORBA 技术引入到以 TMN 为基础的网络管理框架中铺平了道路；X.780 和 Q.816 分别规定了采用细粒度方法的基于 CORBA 技术的网络管理接口定义指南和所需 CORBA 服务；X.780.1 和 Q.816.1 分别规定了采用粗粒度方法的基于 CORBA 技术的网络管理接口定义指南和所需 CORBA 服务。

在 X.780、X.780.1、Q.816 和 Q.816.1 标准的基础之上，已有的 M.3100 和 X.721 规定的信息模型被映射为基于 CORBA 的通用信息模型 M.3120，M.3120 中既包括基于细粒度方式的 CORBA 接口信息模型，也包括基于粗粒度方式的 CORBA 接口信息模型。

基于 X.780、X.780.1、Q.816、Q.816.1 和 M.3120 标准的基础之上，Q.821 中规定的关于报警管理的信息模型被映射为基于 CORBA 的管理信息模型 Q.821.1；Q.822 和 X.739 中规定的关于性能管理的信息模型被映射为基于 CORBA 的管理信息模型 Q.822.1。

在以上基于 CORBA 技术的网络管理接口标准制订过程中，M.3020 这一项建议从规范层面上保证了采用 Q3(用 CMIP 管理协议和 GDMO/ASN.1 描述工具定义的网络管理接口)技术与 CORBA 技术定义接口信息模型时语义的一致性；在 CORBA 接口的实现过程中，X.781 保证了接口的实现和接口规范之间的一致性。

2. 基于 CORBA 技术的网管标准在应用过程中存在的问题

ITU-T SG4 虽然已经完成了 CORBA 技术应用于网络管理中的基础性标准的制定工作，但是该标准要在网管系统的建设到实际应用还必须注意以下几个问题：

(1) TMN 的一致性问题

CORBA 技术的引进扩展了 TMN 的内容，相应的关于 TMN 的一致性和顺从性也必须重新规定。目前，在 CORBA 技术的应用过程中应该重点关注以下几个方面的一致性：

- 涉及 CORBA 互联互通的通信协议的一致性。这主要是指 CORBA 产品中的 ORB 与 OMG CORBA 规范版本的一致性问题。
- 管理框架的一致性。主要是指自定义规范对 X.780、X.780.1、Q.816 和 Q.861.1 中规定的管理框架和管理对象定义指南的支持情况。值得注意的是，本框架中定义了两种管理对象的实现方法，即基于粗粒度和基于细粒度的管理对象实现方法，其一致性也要加以区分。
- 管理框架所需 CORBA 服务的一致性。这主要是指支持 Q.816 和 Q.861.1 中规定的一系列支持该框架的 CORBA 服务的产品的一致性，对于从 OMG 规范中直接引用的 CORBA 服务应该遵循相关的版本规定，对于在本框架内自定义的 CORBA 服务应该与相关 ITU-T 建议的版本保持一致。
- 管理信息模型的一致性。该一致性问题等同于基于 Q3 接口的管理信息模型一致性的规定。

(2) 基于 CORBA 技术的管理接口的复杂度问题

X.780、X.780.1、Q.816 和 Q.861.1 中规定的 TMN 框架要求采用 CORBA 技术实现的网络管理接口的功能，应该在语义上等同于基于 Q3 接口技术的实现，因此，为了弥补 CORBA 技术本身在实现网管接口过程中存在的缺陷，ITU-T 重新引用或定义了大量 CORBA 服务。这些服务的规定使得 CORBA 接口的实现变得极为复杂，在实现过程中应该研究如何简化基于 CORBA 的 TMN 框架。

(3) 符合 TMN 的 CORBA 产品化问题

目前市场上存在的 CORBA 产品种类繁多，但是由于 OMG 本身不存在对 CORBA 一致性认证的机构，因此 CORBA 产品与 OMG CORBA 规范一致性问题无法得到认证，ORB 的互联互通存在着不完备性。

10.5.1.3　新一代网络管理问题

随着电子与计算机技术的快速进步与发展，电信网、计算机网和有线电视网的不断融合，新一代网络已成为目前研究的热点和重点。虽然目前对新一代网络的体系结构、业务质量模型、采用的协议和技术等尚不清楚，但一个公认的观点是新一代网络应拥有先进的强大的网络管理能力。为了保证新一代网络的正常运行，发挥新一代网络的作用，需要对新一代网络进行有效的管理，功能强大的网络管理系统应成为新一代网络的重要组成部分。网络管理系统不仅仅是保证新一代网络正常运行的基本条件，也是保证网络高效、可靠、经济和安全运行的条件，而且新一代网络的一些特性(如：网络智能、网络业务质量保证和网络安全保证等的使用)在很大程度上也取决于相应网络管理系统的能力和质量。因此在研究新一代网络的同时，必须着重研究新一代网络的管理技术。

目前，急需给出解决方案的是对传统的电信网和 IP 网的综合管理问题，ITU-T 和 IETF 已经充分认识到该问题的严重性，两者已经在技术上达成如下共识：

- ITU-T 已经同意在 Q 接口中引进已经被普遍采用的 SNMP 网络管理协议，并根据电信领域的实际需求对原有的 SNMP 协议进行增强。
- IETF 已经认识到 SNMP 体系结构的不足，并同意吸收 TMN 的思想，以支持对电信级网络的管理。

同时，ITU-T 同意 TMF 提出的新一代 OSS 的概念是对 TMN 的补充，特别是在网元管理层和网络管理层标准无法迅速得到贯彻的情况下，按照 TMF 新一代 OSS 的框架进行业务管理层和事务管理层的建设具有十分重要的现实意义。

10.5.2　典型例题分析

例　简述 TMN 的体系结构。

分析：详见 10.5.1.1 节。

答案：ITU-T 从三个方面定义了 TMN 的体系结构(Architecture)，即功能体系结构(Functional Architecture)、信息体系结构(Information Architecture)和物理体系结构(Physical Architecture)。它们分别体现在管理功能块的划分、信息交互的方式和网管的物理实现。按 TMN 的标准从这三个方面出发，对 TMN 系统的结构进行设计。

功能体系结构是从逻辑上描述 TMN 内部的功能分布，引入了一组标准的功能块(Functional block)和可能发生信息交换的参考点(reference points)。整个 TMN 系统即是各种功能块的组合。

信息体系结构包括两个方面：管理信息模型和管理信息交换。管理信息模型是对网络资源及其所支持的管理活动的抽象表示；网络管理功能即是在信息模型的基础上实现的。管理信息交换主要涉及到 TMN 的数据通信功能和消息传递功能，即各物理实体和功能实体之间的通信。

物理体系结构是为实现 TMN 的功能所需的各种物理实体的组织结构。TMN 功能的实现依赖于具体的物理体系结构，从功能体系结构到物理体系结构存在着映射关系。物理体系结构随具体情况的不同而千差万别。在物理体系结构和功能体系结构之间有一定的映射关系。物理体系结构中的一个物理块实现了功能体系结构中的一个或多个功能块，一个接

口实现了功能体系结构中的一组参考点。

10.5.3 同步练习

比较基于 TMN 的网络管理和基于 CORBA 的网络管理的各自优势。

10.5.4 同步练习参考答案

TMN 有技术上的先进、强调公认的标准和接口等优点。TMN 适用于网元层、网元管理层和网络管理层的管理应用。但它也有目标太大、抽象化要求太高、信息模型的标准化进程太慢、OSI 协议栈的效率不高等问题。目前，OMG 的公共对象请求代理体系结构(CORBA)技术越来越被电信、网络部门接受和采用。CORBA 体系结构是对象管理组织 OMG 为解决分布式处理环境中，硬件和软件系统的互联而提出的一种解决方案。CORBA 适用于业务层和事务层的管理应用。

10.6 网 格 计 算

10.6.1 考点辅导

10.6.1.1 什么是网格计算

随着超级计算机的不断发展，它已经成为复杂科学计算领域的主宰。但以超级计算机为中心的计算模式存在明显的不足，而且目前正在经受挑战。超级计算机虽然是一台处理能力强大的“巨无霸”，但它造价极高，通常只有一些国家级的部门，如航天、气象等部门才有能力配置这样的设备。而随着人们日常工作遇到的商业计算越来越复杂，人们越来越需要数据处理能力更强大的计算机，而超级计算机的价格显然阻止了它进入普通人的工作领域。于是，人们开始寻找一种造价低廉而数据处理能力超强的计算模式，最终科学家们找到了答案——网格计算(Grid Computing)。

网格计算是伴随着互联网而迅速发展起来的，专门针对复杂科学计算的新型计算模式。这种计算模式是利用互联网把分散在不同地理位置的计算机组织成一个“虚拟的超级计算机”，其中每一台参与计算的计算机就是一个“节点”，而整个计算是由成千上万个“节点”组成的“一张网格”，所以这种计算方式叫网格计算。这样组织起来的“虚拟的超级计算机”有两个优势，一个是数据处理能力超强；另一个是能充分利用网上的闲置处理能力。

网格计算的目的是，通过任何一台计算机都可以获得无限的计算能力，可以接入浩如烟海的信息。这种环境将能够使企业解决以前难以处理的问题，最有效地使用他们的系统，满足客户要求并降低计算机资源的拥有和管理总成本。网格计算的主要目的是设计一种能够提供以下功能的系统：

- 提高或拓展型企业内所有计算资源的效率和利用率，满足最终用户的需求，同时能够解决以前由于计算、数据或存储资源的短缺而无法解决的问题。
- 建立虚拟组织，通过让它们共享应用和数据来对公共问题进行合作。

- 整合计算能力、存储和其他资源，能使得需要大量计算资源的巨大问题求解成为可能。
- 通过对这些资源进行共享、优化和整体管理，能够降低计算的总成本。

为了促进网格计算的广泛应用，实现让用户随心所欲地共享网格计算中的各种资源，还必须解决以下问题：

- 要解决目前互联网的数据传输能力不足的问题。
- 要进一步解决人机通信的问题。
- 要解决网格上资源共享中的知识产权问题。
- 要保障网格计算的安全性。

10.6.1.2　网格计算系统的特性

1. 分布性和异构性

网格的分布性是指网格的资源是分布的，网格系统由分布在 Internet 上的各类资源组成，包括各类主机、工作站甚至 PC 机，因此网格计算必然是分布的。异构性是指网格计算可运行在 UNIX/NT 等各种操作系统下，也可以是上述机型的机群系统、大型存储设备、数据库或其他设备。怎样实现异构机器之间的协作和转换是网格计算的首要问题。

2. 共享性

网格资源虽然是分布的，但它们却是可以充分共享的(包括软、硬件)，共享是网格的目的，没有共享就没有网格。分布是网格硬件在物理上的特征，而共享是在网格软件支持下实现的逻辑上的特征。

3. 扩展性

元计算系统初期的计算规模较小，随着超级计算机系统的不断加入，系统的计算规模也随之扩大。网格计算系统能够在网格资源规模不断扩大、应用不断增长的情况下，不致降低网格计算的性能。

4. 动态性和结构不可预测性

与一般局域网系统和单机的结构不同，网格计算系统由于地域分布和系统的复杂性以及资源共享，整体结构经常变化。

5. 自适应性

在网格计算中，某一资源出现故障或失败的可能性较高，资源管理必须能动态监视和管理。

6. 自治性和多重管理

由于构成网格计算系统的超级计算资源通常属于不同的机构或组织，使用不同的安全机制，因此网格资源的拥有者对他的资源具有最高级别的管理权限，同时需要不同的机构或组织共同参与网格的统一管理。

10.6.2　典型例题分析

例　列举网格计算系统的特性。

分析：详见 10.6.1.3 节。

答案：分布性、异构性、共享性、扩展性、动态性、结构不可预测性、自适应性、自治性和多重管理。

10.6.3 同步练习

1. 什么是网格？什么是网格计算？
2. 网格的特点。

10.6.4 同步练习参考答案

1. 网格(grid)是一个集成的计算与资源环境，或是说是一个计算资源池。
   网格计算(grid computing)是基于网格的问题求解。
2. 分布与共享；自相似性；动态性与多样性；自治性与管理的多重性。

10.7 本 章 小 结

本章主要要求考生了解和掌握一些网络新技术的概念、特点和应用，这些新技术包括光纤网、无线网、主干网、通信服务、网络管理和网格计算等多方面。

本章的每小节中组织了针对水平考试的典型例题分析和同步练习，这些题目涵盖了大纲规定的知识要点。这些题目将有助于理解和掌握大纲中的知识点。

参 考 文 献

1. 全国计算机技术与软件专业技术资格(水平)考试办公室编. 网络工程师考试大纲. 北京：清华大学出版社，2004
2. 雷振甲编著. 网络工程师教程. 北京：清华大学出版社，2004
3. 周常庆译. 网络分析与设计. 北京：中国电力出版社，2000
4. 胡道元主编. 网络设计师教程. 北京：清华大学出版社，2001
5. 吴国新，吉逸编著. 计算机网络. 南京：东南大学出版社，2000
6. 郭学理主编. 网络设计师教程同步辅导. 北京：清华大学出版社，2001
7. 曾明，李建军等编著. 网络工程与网络管理. 北京：电子工业出版社，2003
8. 何杰等编著. 高速计算机网络 FDDI 技术与应用. 北京：电子工业出版社，1996
9. 刘锦德，刘后铭等编著. 计算机网络大全. 北京：电子工业出版社，1997
10. 鲁士文编著. 计算机网络习题与解析. 北京：清华大学出版社，2001
11. 申普兵主编. 宽带网络技术. 北京：人民邮电出版社，2004
12. Neil P.Reid 著；廖建新译. 宽带固定无线网. 北京：人民邮电出版社，2004
13. (美)Terry William Ogletree 著；李志等译. 网络升级与维护大全. 北京：机械工业出版社，2002
14. 陈明编著. 网络设计教程. 北京：清华大学出版社，2004
15. 李瑞泽编著. Red Hat Linux 7.2 系统管理. 北京：清华大学出版社，2002
16. 陈锦章主编. 宽带 IP 网络技术. 北京：清华大学出版社，2003
17. 赵庆斌，马紫霞，赵庆玉著. 网络测试深入解析. 北京：清华大学出版社，2003
18. 郭军编著. 网络管理. 北京：北京邮电大学出版社，2001
19. 魏大新，李育龙编著. Cisco 网络技术教程. 北京：电子工业出版社，2004
20. 思科系统公司著. 网络互联技术手册. 北京：电子工业出版社，2002
21. 金纯编著. IEEE 802.11 无线局域网. 北京：电子工业出版社，2004
22. 都志辉，陈渝等编著. 网络计算. 北京：清华大学出版社，2002
23. 亿易电脑技术有限责任公司编著. Cisco 网络故障排除仿真试题及精解. 北京：人民邮电出版社，2002
24. (美) Brian Morgan, Craig Dennis 著；张宜春等译. CCNP BCRAN 认证考试(642-821)指南. 北京：人民邮电出版社，2004
25. (美)Diane Teare 编著. CCDA 自学指南. 北京：人民邮电出版社，2004
26. 雷振甲编著. 计算机网络管理及系统开发. 北京：电子工业出版社，2002
27. 蔡建新编著. Cisco CCNP/CCIP 网络工程师. 北京：清华大学出版社，2004
28. Uyless Black 著. ATM 网互通技术(影印版). 北京：清华大学出版社/Prentice Hall 公司，1998
29. Hill Associates,Inc. 著；韩柯译. 电信技术实用指南. 北京：清华大学出版社，2003
30. Bill Burton 著；戴锋译. Cisco 网络远程访问. 北京：机械工业出版社，2001
31. 邵裕忠主编. 电子商务应用开发技术. 北京：高等教育出版社，2000
32. 柴晓路等编著. Web Services 技术、架构和应用. 北京：电子工业出版社，2003

33. James Snell, Doug Tidwell, Pavel Kulchenko著；胡军译. SOAP Web 服务开发. 北京：中国电力出版社，2002
34. David A. Chappell, Tyler Jewell著；毛世杰等译. Java Web 服务. 北京：中国电力出版社，2003
35. (美) A1 Williams 著；何雄等译. Java 2 网络协议内幕. 北京：中国水利水电出版社，2002
36. (美) Douglas E.Comer著；林瑶等译. 用 TCP/IP 进行网际互联第一卷：原理、协议与结构(第四版). 北京：电子工业出版社，2001
37. (美) Ed Roman著；刘晓华译. 精通 EJB(第二版). 北京：电子工业出版社，2002

全国计算机技术与软件专业资格(水平)考试真题及答案

2008 年下半年试题分析与解答 软考指定用书 清华出版(含各科)

2008 年上半年试题分析与解答 软考指定用书 清华出版(含各科)

2007 年下半年试题分析与解答 软考指定用书 清华出版(含各科)

2007 年上半年试题分析与解答 软考指定用书 清华出版(含各科)

2006 年下半年试题分析与解答 软考指定用书 清华出版(含各科)

2006 年上半年试题分析与解答 软考指定用书 清华出版(含各科)

2009 年计算机技术与软件水平考试各科目考试大纲汇总

全国计算机技术与软件专业资格(水平)考试真题及答案汇总

[软考视频]计算机技术与软件专业资格考试推荐视频教程下载汇总

教材及同步辅导见下页。

计算机技术与软件专业技术(水平)考试指定教材及同步辅导

软考初级：

程序员教程(第二版)2007 版 软考指定用书 高清PDF版

程序员考试辅导：全国计算机技术与软件专业技术资格(水平)考试辅导用书

网络管理员教程(第 2 版)2007 版 软考指定用书 高清PDF版

网络管理员考试同步辅导(计算机与网络基础知识篇) 软考指定辅导用书

网络管理员考试同步辅导(网络系统管理与维护篇) 软考指定使用辅导用书

软考中级：

网络工程师教程(第 2 版) 2007 版 软考指定用书 高清PDF版

网络工程师教程 软考指定用书 高清PDF版

网络工程师考试同步辅导：计算机与网络知识篇 软考指定用书

网络工程师考试同步辅导(网络系统设计与管理篇) 软考指定辅导用书

软件设计师教程(第 2 版) 2007 版 软考指定用书 高清PDF版

软件设计师考试同步辅导(下午科目) 高清PDF版

软件设计师考试同步辅导(上午科目) 高清PDF版

软件设计师考试考点分析与真题详解(软件设计技术篇)

软件设计师考试辅导：考点精讲、例题分析、强化训练 冶金工业出版

数据库系统工程师教程 软考指定用书 高清PDF版

软件评测师教程 软考指定教材 高清PDF版

信息系统管理工程师教程 软考指定用书 高清PDF版

信息系统监理师教程 软考指定用书 高清PDF版

软考高级：

系统分析师教程 软考指定教材 高清PDF版

系统分析师考试辅导(2007 版) 软考指定辅导用书 高清PDF版

系统分析师教程 PDF文字版

系统分析师经典教材 Word版

信息系统项目管理师教程 软考指定教材 高清PDF版

信息系统项目管理师辅导教程(上下册)

计算机专业英语教程 PDF文字版

全国计算机技术与软件专业技术资格（水平）考试参考用书

根据人事部、信息产业部文件，计算机技术与软件专业技术资格（水平）考试纳入全国专业技术人员职业资格证书制度的统一规划。通过考试获得证书的人员，表明其已具备从事相应专业岗位工作的水平和能力，用人单位可根据工作需要从获得证书的人员中择优聘任相应专业技术职务（技术员、助理工程师、工程师、高级工程师）。计算机技术与软件专业实施全国统一考试后，不再进行相应专业技术职务任职资格的评审工作。

本系列推荐书目

程序员考试同步辅导（计算机软硬件基础知识篇）
程序员考试同步辅导（程序设计篇）
网络管理员考试同步辅导（计算机与网络基础知识篇）
网络管理员考试同步辅导（网络系统管理与维护篇）
网络工程师考试同步辅导（计算机与网络知识篇）
网络工程师考试同步辅导（网络系统设计与管理篇）

ISBN 7-302-11110-3
9 787302 111108 >
定价：26.00元